تكوين IOS إلى IOS IPSec باستخدام تشفير AES

المحتويات

المقدمة

يقدم هذا المستند نموذجا لتكوين نفق IOS إلى IOS IPSec باستخدام تشفير معيار التشفير المتقدم (AES).

المتطلبات الأساسية

المتطلبات

تم إدخال دعم تشفير AES في برنامج Cisco IOS® 12.2(13)T.

المكونات المستخدمة

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

- برنامج IOS الإصدار 12.3(10) من Cisco
- الموجهات 1721 من Cisco

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

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، ارجع إلى اصطلاحات تلميحات Cisco التقنية.

التكوين

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

ملاحظة: للعثور على معلومات إضافية حول الأوامر المستخدمة في هذا المستند، أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط).

التكوينات

يستخدم هذا المستند التكوينات الموضحة هنا.

- الموجه A-1721
- الموجه B-1721

الموجه A-1721

```
R-1721-A#show run
...Building configuration

Current configuration : 1706 bytes
!
Last configuration change at 00:46:32 UTC Fri Sep 10 !
2004
NVRAM config last updated at 00:45:48 UTC Fri Sep 10 !
2004
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R-1721-A
!
boot-start-marker
boot-end-marker
!
!
memory-size iomem 15
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
no aaa new-model
ip subnet-zero
ip cef
!
!
!
ip audit po max-events 100
no ip domain lookup
no ftp-server write-enable
!
!
!
!

Define Internet Key Exchange (IKE) policy. crypto ---!
isakmp policy 10
```

```
 Specify the 256-bit AES as the !--- encryption ---!
       algorithm within an IKE policy. encr aes 256
Specify that pre-shared key authentication is used. ---!
                              authentication pre-share

    Specify the shared secret. crypto isakmp key ---!
                        cisco123 address 10.48.66.146
                                                    !
                                                    !
    Define the IPSec transform set. crypto ipsec ---!
          transform-set aesset esp-aes 256 esp-sha-hmac
                                                    !
Define crypto map entry name "aesmap" that will use ---!
  !--- IKE to establish the security associations (SA).
                     crypto map aesmap 10 ipsec-isakmp
  Specify remote IPSec peer. set peer 10.48.66.146 ---!
 Specify which transform sets !--- are allowed for ---!
       this crypto map entry. set transform-set aesset
 Name the access list that determines which traffic ---!
!--- should be protected by IPSec. match address acl_vpn
                                                    !
                                                    !
                                                    !
                                          interface ATM0
                                          no ip address
                                               shutdown
                                     no atm ilmi-keepalive
                                    dsl equipment-type CPE
                dsl operating-mode GSHDSL symmetric annex A
                                        dsl linerate AUTO
                                                    !
                                       interface Ethernet0
                        ip address 192.168.100.1 255.255.255.0
                                          ip nat inside
                                            half-duplex
                                                    !
                                    interface FastEthernet0
                         ip address 10.48.66.147 255.255.254.0
                                        ip nat outside
                                            speed auto
    Apply crypto map to the interface. crypto map ---!
                                                aesmap
                                                    !
               ip nat inside source list acl_nat interface
                                        FastEthernet0 overload
                                                ip classless
                            ip route 0.0.0.0 0.0.0.0 10.48.66.1
    ip route 192.168.200.0 255.255.255.0 FastEthernet0
                                        no ip http server
                                    no ip http secure-server
                                                    !


                                 ip access-list extended acl_nat
  Exclude protected traffic from being NAT'ed. deny ---!
      ip 192.168.100.0 0.0.0.255 192.168.200.0 0.0.0.255
                    permit ip 192.168.100.0 0.0.0.255 any

    Access list that defines traffic protected by ---!
                    IPSec. ip access-list extended acl_vpn
        permit ip 192.168.100.0 0.0.0.255 192.168.200.0
                                                0.0.0.255
                                                    !
                                                    !
```

```
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
!
end

#R-1721-A
```

الموجه B-1721

```
R-1721-B#show run
...Building configuration

Current configuration : 1492 bytes
!
Last configuration change at 14:11:41 UTC Wed Sep 8 !
2004
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R-1721-B
!
boot-start-marker
boot-end-marker
!
!
memory-size iomem 15
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
no aaa new-model
ip subnet-zero
ip cef
!
!
!
ip audit po max-events 100
no ip domain lookup
no ftp-server write-enable
!
!
!
!
!
Define IKE policy. crypto isakmp policy 10 ---!
Specify the 256-bit AES as the !--- encryption ---!
algorithm within an IKE policy. encr aes 256
Specify that pre-shared key authentication is used. ---!
authentication pre-share

Specify the shared secret. crypto isakmp key ---!
cisco123 address 10.48.66.147
!
!
Define the IPSec transform set. crypto ipsec ---!
transform-set aesset esp-aes 256 esp-sha-hmac
!
Define crypto map entry name "aesmap" that uses !-- ---!
```

```
 - IKE to establish the SA. crypto map aesmap 10 ipsec-
                                                    isakmp
  Specify remote IPSec peer. set peer 10.48.66.147 ---!
  Specify which transform sets !--- are allowed for ---!
        this crypto map entry. set transform-set aesset
 Name the access list that determines which traffic ---!
!--- should be protected by IPSec. match address acl_vpn
                                                        !
                                                        !
                                                        !
                                        interface Ethernet0
                ip address 192.168.200.1 255.255.255.0
                                             ip nat inside
                                               half-duplex
                                                        !
                                    interface FastEthernet0
                 ip address 10.48.66.146 255.255.254.0
                                           ip nat outside
                                               speed auto
     Apply crypto map to the interface. crypto map ---!
                                                  aesmap
                                                        !
           ip nat inside source list acl_nat interface
                                    FastEthernet0 overload
                                             ip classless
                    ip route 0.0.0.0 0.0.0.0 10.48.66.1
     ip route 192.168.100.0 255.255.255.0 FastEthernet0
                                        no ip http server
                                  no ip http secure-server
                                                        !
                             ip access-list extended acl_nat
 Exclude protected traffic from being NAT'ed.  deny ---!
     ip 192.168.200.0 0.0.0.255 192.168.100.0 0.0.0.255
                  permit ip 192.168.200.0 0.0.0.255 any


     Access list that defines traffic protected by ---!
                  IPSec. ip access-list extended acl_vpn
       permit ip 192.168.200.0 0.0.0.255 192.168.100.0
                                                0.0.0.255
                                                        !
                                                        !
                                               line con 0
                                        exec-timeout 0 0
                                               line aux 0
                                            line vty 0 4
                                                        !
                                                      end

                                                #R-1721-B
```

التحقق من الصحة

يوفر هذا القسم معلومات يمكنك إستخدامها للتأكد من أن التكوين يعمل بشكل صحيح.

يتم دعم بعض أوامر **العرض بواسطة** أداة مترجم الإخراج (العملاء المسجلون فقط)، والتي تتيح لك عرض تحليل إخراج أمر **العرض**.

- **show crypto isakmp sa**—يعرض حالة بروتوكول إدارة المفاتيح وارتباط أمان الإنترنت (ISAKMP) SA.
- **show crypto ipsSA** — يعرض الإحصائيات على الأنفاق النشطة.

- **show crypto engine connections active**—يعرض إجمالي التشفيرات/فك التشفير لكل SA.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

أوامر استكشاف الأخطاء وإصلاحها

ملاحظة: قبل إصدار أوامر **تصحيح الأخطاء**، يرجى الاطلاع على المعلومات المهمة في أوامر تصحيح الأخطاء.

- **debug crypto ipSec**—يعرض أحداث IPSec.
- **debug crypto isakmp**—يعرض الرسائل المتعلقة بأحداث IKE.
- **debug crypto engine**—يعرض معلومات من محرك التشفير.

يمكن العثور على معلومات إضافية حول أستكشاف أخطاء IPSec وإصلاحها في أستكشاف أخطاء أمان IP وإصلاحها - فهم أوامر تصحيح الأخطاء واستخدامها.

معلومات ذات صلة

- برنامج IOS الإصدارات 12.2T من Cisco - معيار التشفير المتقدم (AES)
- تكوين أمان شبكة IPSec
- صفحة دعم IPSec
- الدعم الفني - 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).