IPSec عبر تكوينات عينة الكبلات وتصحيح الأخطاء

المحتويات

المقدمة

أمان بروتوكول الإنترنت (IPsec) هو إطار عمل للمعايير المفتوحة يضمن الاتصالات الخاصة الآمنة عبر شبكات IP. استنادا إلى المعايير التي تم تطويرها بواسطة "فريق العمل الهندسي" (IETF) عبر الإنترنت، يضمن بروتوكول IPsec سرية إتصالات البيانات عبر شبكة IP العامة وسلامتها وأصالتها. يوفر IPsec مكونا ضروريا لحل مرن قائم على المعايير لنشر سياسة أمان على مستوى الشبكة.

يقدم هذا المستند مثالا للتكوين IPsec بين جهازي مودم كبل Cisco. يقوم هذا التكوين بإنشاء نفق تشفير عبر شبكة كبل بين موجهات مودم كبل Cisco uBR9xx Series. يتم تشفير جميع حركات مرور البيانات بين الشبكتين. ولكن يسمح لحركة المرور الموجهة للشبكات الأخرى بالمرور دون تشفير. بالنسبة لمستخدمي المكاتب الصغيرة والمكاتب المنزلية (SOHO)، يتيح ذلك إنشاء الشبكات الخاصة الظاهرية (VPN) عبر شبكة كبلات.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

يجب أن تتوافق أجهزة المودم مع هذه المتطلبات لتكوين IPsec على أجهزة مودم الكبل:

- Cisco uBR904، uBR905، أو uBR924 في وضع التوجيه
- مجموعة ميزات IPsec 56

- برنامج IOS® الإصدار 12.0(5)T من Cisco أو إصدار أحدث

وبالإضافة إلى ذلك، يجب أن يكون لديك نظام توصيل مودم الكبل (CMTS)، وهو أي جهاز توجيه لكبلات وحدة الاستقبال والبث عبر الكبلات (DOCSIS) متوافق مع مواصفات واجهة خدمة البيانات المنقولة عبر الكبلات، مثل Cisco uBR7246 أو Cisco uBR7223 أو Cisco uBR7246VXR.

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.

النظرية الأساسية

يستخدم المثال الموجود في هذا المستند مودم كبل uBR904، ومودم كبل uBR924، و uBR7246VXR CMTS. تقوم أجهزة مودم الكبل بتشغيل برنامج Cisco IOS الإصدار 12.1(6)، ويقوم CMTS بتشغيل برنامج Cisco IOS الإصدار 12.1(4)EC.

ملاحظة: يتم تنفيذ هذا المثال باستخدام التكوين اليدوي على أجهزة مودم الكبلات من خلال منفذ وحدة التحكم. إذا تم تنفيذ عملية مؤتمتة من خلال ملف تكوين DOCSIS (يتم إنشاء البرنامج النصي ios.cfg باستخدام تكوين IPsec) *فلا* يمكن إستخدام قوائم الوصول *100 و 101*. وذلك لأن تنفيذ Cisco لجدول DocsDevNmAccess لبروتوكول إدارة الشبكة البسيط (SNMP) يستخدم قوائم وصول Cisco IOS. وهو يقوم بإنشاء قائمة وصول واحدة لكل واجهة. في uBR904 و 924 و 905، يتم إستخدام قائمتي الوصول الأوليين بشكل عام (100 و 101). على مودم كبل يدعم الناقل التسلسلي العالمي (USB)، مثل CVA120، يتم إستخدام ثلاث قوائم وصول (100، 101، و 102).

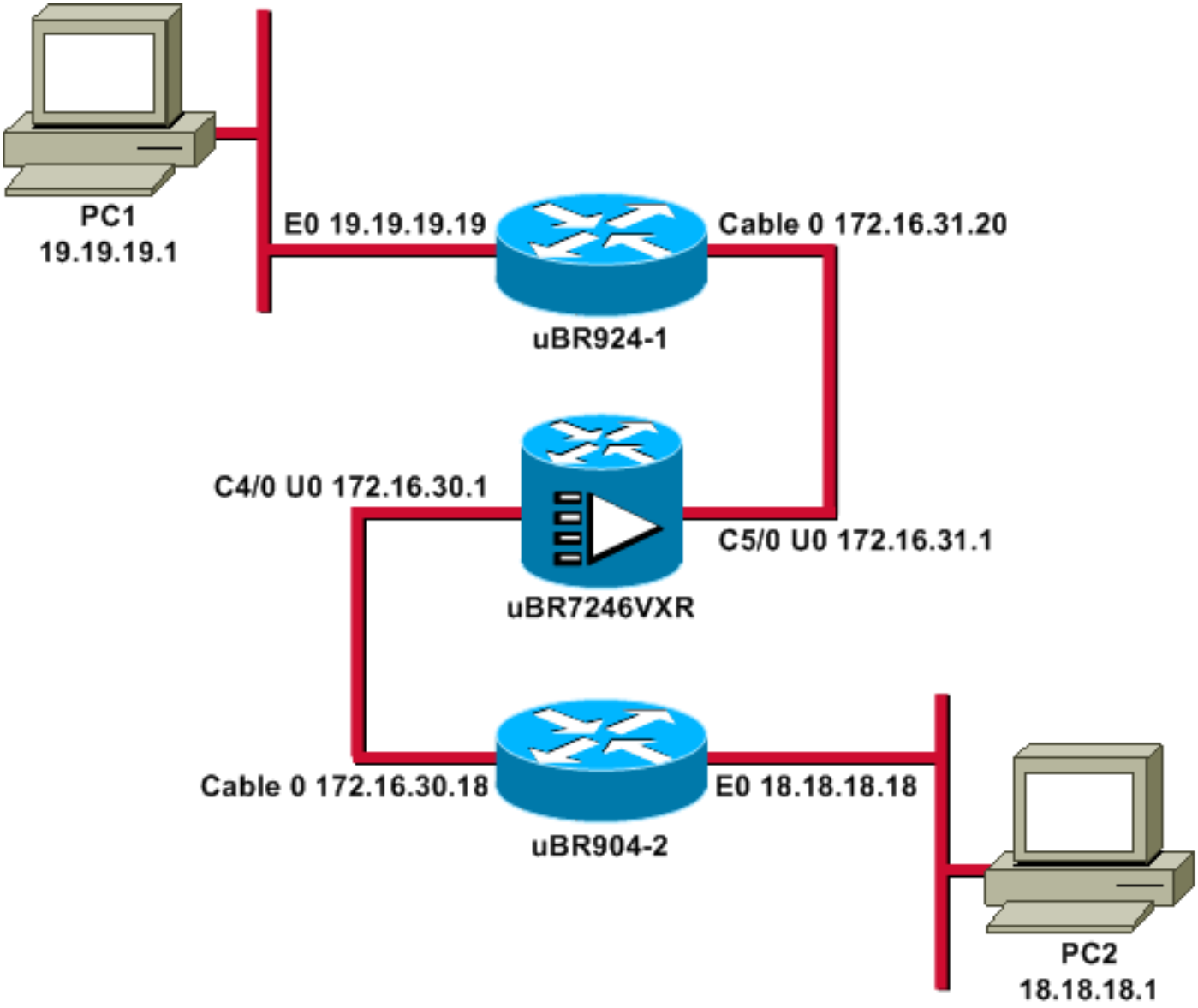
التكوين

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

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

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



ملاحظة: تحتوي جميع عناوين IP في هذا المخطط على قناع 24 بت.

التكوينات

يستخدم هذا المستند التكوينات التالية:

- uBR924-1
- uBR904-2
- uBR7246VXR

uBR924-1

```
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ubr924-1
!
enable password ww
!
!
!
```

```
!
clock timezone - -8
ip subnet-zero
no ip finger
!
ip audit notify log
ip audit po max-events 100
!
!
crypto isakmp policy 10
Creates an Internet Key Exchange (IKE) policy with ---!
the specified priority !--- number of 10. The range for
the priority is 1 to 10000, where 1 is the !--- highest
priority. This command also enters Internet Security
Association !--- and Key Management Protocol (ISAKMP)
policy configuration command mode. hash md5
Specifies the MD5 (HMAC variant) hash algorithm for ---!
packet authentication. authentication pre-share
Specifies that the authentication keys are pre- ---!
shared, as opposed to !--- dynamically negotiated using
Rivest, Shamir, and Adelman (RSA) public !--- key
signatures. group 2
Diffie-Hellman group for key negotiation. lifetime ---!
3600
Defines how long, in seconds, each security ---!
association should exist before !--- it expires. Its
range is 60 to 86400, and in this case, it is 1 hour.
crypto isakmp key mykey address 18.18.18.18
Specifies the pre-shared key that should be used ---!
with the peer at the !--- specific IP address. The key
can be any arbitrary alphanumeric key up to !--- 128
characters. The key is case-sensitive and must be
entered identically !--- on both routers. In this case,
the key is mykey and the peer is the !--- Ethernet
address of uBR904-2
.
!
crypto IPSec transform-set TUNNELSET ah-md5-hmac esp-des
Establishes the transform set to use for IPsec ---!
encryption. As many as !--- three transformations can be
specified for a set. Authentication Header !--- and ESP
are in use. Another common transform set used in
.industry is !--- esp-des esp-md5-hmac


!
crypto map MYMAP local-address Ethernet0
Creates the MYMAP crypto map and applies it to the ---!
.Ethernet0 interface


crypto map MYMAP 10 ipsec-isakmp
Creates a crypto map numbered 10 and enters crypto ---!
map configuration mode. set peer 18.18.18.18
Identifies the IP address for the destination peer ---!
router. In this case, !--- the Ethernet interface of the
remote cable modem (ubr904-2) is used. set transform-set
TUNNELSET
Sets the crypto map to use the transform set ---!
previously created. match address 101
Sets the crypto map to use the access list that ---!
specifies the type of !--- traffic to be encrypted. !---
Do not use access lists 100, 101, and 102 if the IPsec
config is !--- downloaded through the ios.cfg in the
.DOCSIS configuration file
```

```
!
!
!
!
voice-port 0
input gain -2
output attenuation 0
!
voice-port 1
input gain -2
output attenuation 0
!
!
!
interface Ethernet0
ip address 19.19.19.19 255.255.255.0
ip rip send version 2
ip rip receive version 2
no ip route-cache
no ip mroute-cache
!
interface cable-modem0
ip rip send version 2
ip rip receive version 2
no ip route-cache
no ip mroute-cache
cable-modem downstream saved channel 525000000 39 1
cable-modem mac-timer t2 40000
no cable-modem compliant bridge
crypto map MYMAP
 Applies the previously created crypto map to the ---!
cable interface. ! router rip version 2 network 19.0.0.0
network 172.16.0.0 ! ip default-gateway 172.16.31.1 ip
classless ip http server ! access-list 101 permit ip
19.19.19.0 0.0.0.255 18.18.18.0 0.0.0.255
 Access list that identifies the traffic to be ---!
encrypted. In this case, !--- it is setting traffic from
the local Ethernet network to the remote !--- Ethernet
network. snmp-server manager ! line con 0 transport
input none line vty 0 4 password ww login ! end
```

تكوين مودم الكبل الآخر مماثل جدا، لذلك يتم حذف معظم التعليقات في التكوين السابق.

uBR904-2

```
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ubr904-2
!
enable password ww
!
!
!
!
!
clock timezone - -8
ip subnet-zero
no ip finger
```

```
!
!
!
crypto isakmp policy 10
hash md5
authentication pre-share
group 2
lifetime 3600
crypto isakmp key mykey address 19.19.19.19
!
!
crypto IPSec transform-set TUNNELSET ah-md5-hmac ESP-Des
!
crypto map MYMAP local-address Ethernet0
crypto map MYMAP 10 ipsec-isakmp
set peer 19.19.19.19
 Identifies the IP address for the destination peer ---!
router. In this case, !--- the Ethernet interface of the
remote cable modem (uBR924-1) is used. set transform-set
TUNNELSET
match address 101
!
!
!
!
interface Ethernet0
ip address 18.18.18.18 255.255.255.0
ip rip send version 2
ip rip receive version 2
!
interface cable-modem0
ip rip send version 2
ip rip receive version 2
no keepalive
cable-modem downstream saved channel 555000000 42 1
cable-modem Mac-timer t2 40000
no cable-modem compliant bridge
crypto map MYMAP
!
router rip
version 2
network 18.0.0.0
network 172.16.0.0
!
ip default-gateway 172.16.30.1
ip classless
no ip http server
!
access-list 101 permit ip 18.18.18.0 0.0.0.255
19.19.19.0 0.0.0.255
snmp-server manager
!
line con 0
transport input none
line vty 0 4
password ww
login
!
end
```

كما يشغل CMTS uBR7246VXR بروتوكول معلومات التوجيه (RIP) الإصدار 2، وبالتالي يعمل التوجيه. هذا ال rip تشكيل يستعمل على ال CMTS:

uBR7246VXR
router rip version 2 network 172.16.0.0 no auto-summary

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

للتحقق من عمل IPsec:

- تحقق من هذه الأشياء:يدعم برنامج Cisco IOS برنامج IPsec.التكوين الجاري تشغيله صحيح.الواجهات قيد التشغيل.يعمل التوجيه.قائمة الوصول المعرفة لتشفير حركة المرور صحيحة.
- قم بإنشاء حركة مرور وانظر إلى التشفير وفك التشفير، لترى المقدار الذي يتزايد.
- تشغيل تصحيح الأخطاء للتشفير.

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

قم بإصدار الأمر **show version** على كل من أجهزة مودم الكبل.

```
ubr924-1#show version
Cisco Internetwork Operating System Software
,(IOS (tm) 920 Software (UBR920-K1O3SV4Y556I-M), Version 12.1(6
(RELEASE SOFTWARE (fc1
.Copyright (c) 1986-2000 by Cisco Systems, Inc
Compiled Wed 27-Dec-00 16:36 by kellythw
Image text-base: 0x800100A0, data-base: 0x806C1C20

(ROM: System Bootstrap, Version 12.0(6r)T3, RELEASE SOFTWARE (fc1

ubr924-1 uptime is 1 hour, 47 minutes
System returned to ROM by reload at 10:39:05 - Fri Feb 9 2001
System restarted at 10:40:05 - Fri Feb 9 2001
"System image file is "flash:ubr920-k1o3sv4y556i-mz.121-6

(cisco uBR920 CM (MPC850) processor (revision 3.e
.with 15872K/1024K bytes of memory
Processor board ID FAA0422Q04F
.Bridging software
(Ethernet/IEEE 802.3 interface(s 1
(Cable Modem network interface(s 1
(3968K bytes of processor board System flash (Read/Write
(1536K bytes of processor board Boot flash (Read/Write

Configuration register is 0x2102
```

يتم تشغيل uBR924-1 ببرنامج Cisco IOS Software، الإصدار 12.1(6) مع مجموعة ميزات Small Office/Voice/FW IPSec 56 ذات القيمة.

```
ubr904-2#show version
Cisco Internetwork Operating System Software
,(IOS (TM) 900 Software (UBR900-K1OY556I-M), Version 12.1(6
(RELEASE SOFTWARE (fc1
```

```
.Copyright (c) 1986-2000 by cisco Systems, Inc
Compiled Wed 27-DEC-00 11:06 by kellythw
Image text-base: 0x08004000, database: 0x085714DC

ROM: System Bootstrap, Version 11.2(19980518:195057), RELEASED SOFTWARE
,ROM: 900 Software (UBR900-RBOOT-M), Version 11.3(11)NA
(EARLY DEPLOYMENT RELEASE SOFTWARE (fc1

ubr904-2 uptime is 1 hour, 48 minutes
System returned to ROM by reload at 10:38:44 - Fri Feb 9 2001
System restarted at 10:40:37 - Fri Feb 9 2001
"System image file is "flash:ubr900-k1oy556i-mz.121-6

(cisco uBR900 CM (68360) processor (revision D
.with 8192K bytes of memory
Processor board ID FAA0235Q0ZS
.Bridging software
(Ethernet/IEEE 802.3 interface(s 1
(Cable Modem network interface(s 1
(4096K bytes of processor board System flash (Read/Write
(2048K bytes of processor board Boot flash (Read/Write

Configuration register is 0x2102
```

يعمل uBR904-2 ببرنامج Cisco IOS Software، الإصدار 12.1(6) مع مجموعة ميزات Small Office/FW IPSec 56.

```
ubr924-1#show ip interface brief
Interface            IP-Address      OK? Method Status          Protocol
      Ethernet0            19.19.19.19     YES NVRAM  up              up
      cable-modem0         172.16.31.20    YES unset  up              up

ubr904-2#show ip interface brief
Interface            IP-Address      OK? Method Status          Protocol
      Ethernet0            18.18.18.18     YES NVRAM  up              up
      cable-modem0         172.16.30.18    YES unset  up              up
```

من الأمر الأخير، يمكنك أن ترى أن واجهات الإيثرنت قيد التشغيل. تم إدخال عناوين IP لواجهات الإيثرنت يدويا. كما تم رفع واجهات الكبلات وتعلمت تلك الواجهات عناوين IP الخاصة بها من خلال DHCP. نظرا لتخصيص عناوين الكبلات هذه بشكل ديناميكي، فلا يمكن إستخدامها كنظراء في تكوين IPSec.

```
ubr924-1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
   D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
   N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
    E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - ISIS level-1, L2 - ISIS level-2, ia - ISIS inter area
        candidate default, U - per-user static route, o - ODR - *
                    P - periodic downloaded static route

Gateway of last resort is 172.16.31.1 to network 0.0.0.0

                    is subnetted, 1 subnets 19.0.0.0/24
                C       19.19.19.0 is directly connected, Ethernet0
          R    18.0.0.0/8 [120/2] via 172.16.31.1, 00:00:23, cable-modem0
             is variably subnetted, 4 subnets, 3 masks 172.16.0.0/16
 R       172.16.135.0/25 [120/1] via 172.16.31.1, 00:00:23, cable-modem0
  R       172.16.29.0/27 [120/1] via 172.16.31.1, 00:00:23, cable-modem0
  R       172.16.30.0/24 [120/1] via 172.16.31.1, 00:00:23, cable-modem0
            C       172.16.31.0/24 is directly connected, cable-modem0
```

```
R    192.168.99.0/24 [120/3] via 172.16.31.1, 00:00:24, cable-modem0
                     is subnetted, 2 subnets 10.0.0.0/24
R       10.10.10.0 [120/2] via 172.16.31.1, 00:00:24, cable-modem0
S*   0.0.0.0/0 [1/0] via 172.16.31.1
```

يمكنك أن ترى من هذا الإخراج أن uBR924-1 يتعلم حول المسار 18.18.18.0، وهو واجهة إيثرنت ل uBR904-2.

```
ubr904-2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - ISIS, L1 - ISIS level-1, L2 - ISIS level-2, IA - ISIS inter area
       candidate default, U - per-user static route, o - ODR - *
       P - periodic downloaded static route

Gateway of last resort is 172.16.30.1 to network 0.0.0.0

R    19.0.0.0/8 [120/2] via 172.16.30.1, 00:00:17, cable-modem0
                     is subnetted, 1 subnets 18.0.0.0/24
C       18.18.18.0 is directly connected, Ethernet0
     is variably subnetted, 4 subnets, 3 masks 172.16.0.0/16
R       172.16.135.0/25 [120/1] via 172.16.30.1, 00:00:17, cable-modem0
R       172.16.29.224/27 [120/1] via 172.16.30.1, 00:00:17, cable-modem0
C       172.16.30.0/24 is directly connected, cable-modem0
R       172.16.31.0/24 [120/1] via 172.16.30.1, 00:00:17, cable-modem0
R    192.168.99.0/24 [120/3] via 172.16.30.1, 00:00:18, cable-modem0
                     is subnetted, 1 subnets 10.0.0.0/24
R       10.10.10.0 [120/2] via 172.16.30.1, 00:00:18, cable-modem0
S*   0.0.0.0/0 [1/0] via 172.16.30.1
```

من جدول التوجيه الخاص ب uBR904-2، يمكنك أن ترى أن شبكة إيثرنت الخاصة ب uBR924-1 موجودة في جدول التوجيه.

ملاحظة: قد تكون هناك حالات لا يمكنك فيها تشغيل بروتوكول توجيه بين أجهزة مودم الكبل. في مثل هذه الحالات، أنت ينبغي أضفت مسحاج تخديد ساكن إستاتيكي على ال CMTS أن يوجه حركة مرور ل ال إثرنيت قارن من الكبل مودم.

الأمر التالي الذي يجب فحصه هو اعتماد قائمة الوصول؛ قم بإصدار الأمر **show access-lists** على كلا الموجهين.

```
ubr924-1#show access-lists
Extended IP access list 101
(permit ip 19.19.19.0 0.0.0.255 18.18.18.0 0.0.0.255 (2045 matches

ubr904-2#show access-lists
Extended IP access list 101
(permit ip 18.18.18.0 0.0.0.255 19.19.19.0 0.0.0.255 (2059 matches
```

ثبتت قائمة الوصول جلسة IPsec عندما يرسل الشبكة المحلية خلف 19.19.19.0 (uBR924-1) حركة مرور IP إلى الشبكة المحلية خلف 18.18.18.0 (uBR904-2)، والعكس. لا *تستخدم* "any" في قوائم الوصول، لأنها تتسبب في حدوث مشاكل. راجع تكوين أمان شبكة IPsec للحصول على مزيد من التفاصيل.

لا توجد حركة مرور IPsec. قم بإصدار الأمر **show crypto engine connection active**.

```
ubr924-1#show crypto engine connection active
ID Interface    IP-Address   State   Algorithm           Encrypt  Decrypt
set     HMAC_MD5+DES_56_CB      0         0                        1

ubr904-2#show crypto engine connection active
```

```
ID Interface     IP-Address     State     Algorithm           Encrypt  Decrypt
set      HMAC_MD5+DES_56_CB         0         0                                1
```

لا توجد إتصالات IPsec بسبب عدم تطابق أي حركة مرور لقوائم الوصول.

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

تتمثل الخطوة التالية في تشغيل بعض تصحيح أخطاء التشفير لإنشاء حركة مرور مثيرة للاهتمام.

في هذا المثال، يتم تشغيل عمليات تصحيح الأخطاء هذه:

- **محرك تصحيح الأخطاء المشفرة**
- **debug crypto IPsec**
- **debug crypto key-exchange**
- **debug crypto isakmp**

يجب أن تقوم أولا بإنشاء حركة مرور مثيرة للإهتمام لترى مخرجات تصحيح الأخطاء. قم بإصدار إختبار اتصال موسع من منفذ الإيثرنت uBR904-2 إلى الكمبيوتر الشخصي على uBR924-1 (عنوان IP 19.19.19.1).

```
ubr904-2#ping ip
Target IP address: 19.19.19.1
IP address of PC1 behind the Ethernet of uBR924-1. Repeat count [5]: 100 ---!
Sends 100 pings. Datagram size [100]: Timeout in seconds [2]: Extended commands [n]: y ---!
Source address or interface: 18.18.18.18
IP address of the Ethernet behind uBR904-2. Type of service [0]: Set DF bit in IP header? ---!
[no]: Validate reply data? [no]: Data pattern [0xABCD]: Loose, Strict, Record, Timestamp,
Verbose[none]: Sweep range of sizes [n]: Type escape sequence to abort. Sending 100, 100-byte
:ICMP Echos to 19.19.19.1, timeout is 2 seconds
```

يعرض uBR924-2 إخراج تصحيح الأخطاء هذا:

```
ubr904-2#
, :(IPSec(sa_request :01:50:37
,key eng. msg.) src= 18.18.18.18, dest= 19.19.19.19)
,(src_proxy= 18.18.18.0/255.255.255.0/0/0 (type=4
,(dest_proxy= 19.19.19.0/255.255.255.0/0/0 (type=4
, protocol= AH, transform= ah-md5-hmac
,lifedur= 3600s and 4608000kb
spi= 0x19911A16(428939798), conn_id= 0, keysize= 0, flags= 0x4004
, :(IPSec(sa_request :01:50:37
,key Eng. msg.) src= 18.18.18.18, dest= 19.19.19.19)
,(src_proxy= 18.18.18.0/255.255.255.0/0/0 (type=4
,(dest_proxy= 19.19.19.0/255.255.255.0/0/0 (type=4
, protocol= ESP, transform= ESP-Des
,lifedur= 3600s and 4608000kb
spi= 0x7091981(118036865), conn_id= 0, keysize= 0, flags= 0x4004
(ISAKMP: received ke message (1/2 :01:50:37
(ISAKMP (0:1): sitting IDLE. Starting QM immediately (QM_IDLE :01:50:37
ISAKMP (0:1): beginning Quick Mode exchange, M-ID of 1108017901 :01:50:37
CryptoEngine0: generate hmac context for conn id 1 :01:50:37
ISAKMP (1): sending packet to 19.19.19.19 (I) QM_IDLE :01:50:37
ISAKMP (1): received packet from 19.19.19.19 (I) QM_IDLE :01:50:37
CryptoEngine0: generate hmac context for conn id 1 :01:50:37
ISAKMP (0:1): processing SA payload. message ID = 1108017901 :01:50:37
ISAKMP (0:1): Checking IPSec proposal 1 :01:50:37
ISAKMP: transform 1, AH_MD5 :01:50:37
:ISAKMP: attributes in transform :01:50:37
ISAKMP: encaps is 1 :7!!!!!!!!!!!!!!!!!!!!!!!!.01:50:3
ISAKMP: SA life type in seconds :01:50:37
ISAKMP: SA life duration (basic) of 3600 :01:50:37
```

```
ISAKMP:      SA life type in kilobytes :01:50:37
ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0 :01:50:37
ISAKMP:      authenticator is HMAC-MD5 :01:50:37
validate proposal 0 :01:50:37
.ISAKMP (0:1): atts are acceptable :01:50:37
ISAKMP (0:1): Checking IPSec proposal 1 :01:50:37
ISAKMP: transform 1, ESP_DES :01:50:37
:ISAKMP:   attributes in transform :01:50:37
ISAKMP:      encaps is 1 :01:50:37
ISAKMP:      SA life type in seconds :01:50:37
ISAKMP:      SA life duration (basic) of 3600 :01:50:37
ISAKMP:      SA life type in kilobytes :01:50:37
ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0 :01:50:37
validate proposal 0 :01:50:37
.ISAKMP (0:1): atts are acceptable :01:50:37
,IPSec(validate_proposal_request): proposal part #1 :01:50:37
,key Eng. msg.) dest= 19.19.19.19, src= 18.18.18.18)
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!dest_proxy= 19.19.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 99 percent (99/100), round-trip min/avg/max = 30/40/70 ms
ubr904-2#
```

لاحظ أن إختبار الاتصال الأول فشل. وهذا لأنه يحتاج إلى تأسيس الاتصال.

يعرض uBR924-1 إخراج تصحيح الأخطاء هذا:

```
ubr924-1#
ISAKMP (1): received packet from 18.18.18.18 (R) QM_IDLE :01:50:24
CryptoEngine0: generate hmac context for conn id 1 :01:50:24
ISAKMP (0:1): processing SA payload. Message ID = 1108017901 :01:50:24
ISAKMP (0:1): Checking IPSec proposal 1 :01:50:24
ISAKMP: transform 1, AH_MD5 :01:50:24
:ISAKMP:   attributes in transform :01:50:24
ISAKMP:      encaps is 1 :01:50:24
ISAKMP:      SA life type in seconds :01:50:24
ISAKMP:      SA life duration (basic) of 3600 :01:50:24
ISAKMP:      SA life type in kilobytes :01:50:24
ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0 :01:50:24
ISAKMP:      authenticator is HMAC-MD5 :01:50:24
validate proposal 0 :01:50:24
.ISAKMP (0:1): atts are acceptable :01:50:24
ISAKMP (0:1): Checking IPSec proposal 1 :01:50:24
ISAKMP: transform 1, ESP_DES :01:50:24
:ISAKMP:   attributes in transform :01:50:24
ISAKMP:      encaps is 1 :01:50:24
ISAKMP:      SA life type in seconds :01:50:24
ISAKMP:      SA life duration (basic) of 3600 :01:50:24
ISAKMP:      SA life type in kilobytes :01:50:24
ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0 :01:50:24
validate proposal 0 :01:50:24
.ISAKMP (0:1): atts are acceptable :01:50:24
,IPSec(validate_proposal_request): proposal part #1 :01:50:24
,key Eng. msg.) dest= 19.19.19.19, src= 18.18.18.18)
,(dest_proxy= 19.19.19.0/255.255.255.0/0/0 (type=4
,(src_proxy= 18.18.18.0/255.255.255.0/0/0 (type=4
, protocol= AH, transform= ah-md5-hmac
,lifedur= 0s and 0kb
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
,IPSec(validate_proposal_request): proposal part #2 :01:50:24
,key Eng. msg.) dest= 19.19.19.19, src= 18.18.18.18)
,(dest_proxy= 19.19.19.0/255.255.255.0/0/0 (type=4
,(src_proxy= 18.18.18.0/255.255.255.0/0/0 (type=4
, protocol= ESP, transform= ESP-Des
```

```
                                                    ,lifedur= 0s and 0kb
                                spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
                                             validate proposal request 0 :01:50:24
ISAKMP (0:1): processing NONCE payload. Message ID = 1108017901 :01:50:24
   ISAKMP (0:1): processing ID payload. Message ID = 1108017901 :01:50:24
   ISAKMP (1): ID_IPV4_ADDR_SUBNET src 18.18.18.0/255.255.255.0 :01:50:24
                                                           prot 0 Port 0
   ISAKMP (0:1): processing ID payload. Message ID = 1108017901 :01:50:24
   ISAKMP (1): ID_IPV4_ADDR_SUBNET dst 19.19.19.0/255.255.255.0 :01:50:24
                                                           prot 0 Port 0
                          ISAKMP (0:1): asking for 2 spis from IPSec :01:50:24
                             ...IPSec(key_engine): got a queue event :01:50:24
                   IPSec(spi_response): getting spi 393021796 for SA :01:50:24
                    from 18.18.18.18     to 19.19.19.19     for prot 2
                    IPSec(spi_response): getting spi 45686884 for SA :01:50:24
                    from 18.18.18.18     to 19.19.19.19     for prot 3
                                  (ISAKMP: received ke message (2/2 :01:50:24
                      CryptoEngine0: generate hmac context for conn id 1 :01:50:24
                 ISAKMP (1): sending packet to 18.18.18.18 (R) QM_IDLE :01:50:24
              ISAKMP (1): received packet from 18.18.18.18 (R) QM_IDLE :01:50:24
                   CryptoEngine0: generate hmac context for conn id 1 :01:50:24
                                             IPSec allocate flow 0 :01:50:24
                                             IPSec allocate flow 0 :01:50:24
                                  ISAKMP (0:1): Creating IPSec SAs :01:50:24
                  inbound SA from 18.18.18.18 to 19.19.19.19         :01:50:24
                            (proxy 18.18.18.0 to 19.19.19.0)
                has spi 393021796 and conn_id 2000 and flags 4         :01:50:24
                                  lifetime of 3600 seconds         :01:50:24
                               lifetime of 4608000 kilobytes         :01:50:24
                 outbound SA from 19.19.19.19 to 18.18.18.18         :01:50:24
                            (proxy 19.19.19.0 to 18.18.18.0)
                has spi 428939798 and conn_id 2001 and flags 4         :01:50:24
                                  lifetime of 3600 seconds         :01:50:24
                               lifetime of 4608000 kilobytes         :01:50:24
                                  ISAKMP (0:1): Creating IPSec SAs :01:50:24
                  inbound SA from 18.18.18.18 to 19.19.19.19         :01:50:24
                            (proxy 18.18.18.0 to 19.19.19.0)
                 has spi 45686884 and conn_id 2002 and flags 4         :01:50:24
                                  lifetime of 3600 seconds         :01:50:24
                               lifetime of 4608000 kilobytes         :01:50:24
                 outbound SA from 19.19.19.19 to 18.18.18.18         :01:50:24
                            (proxy 19.19.19.0 to 18.18.18.0)
                has spi 118036865 and conn_id 2003 and flags 4         :01:50:24
                                  lifetime of 3600 seconds         :01:50:25
                               lifetime of 4608000 kilobytes         :01:50:25
          ISAKMP (0:1): deleting node 1108017901 error FALSE reason :01:50:25
                                       "()quick mode done (await"
                            ...IPSec(key_engine): got a queue event :01:50:25
                                                  , :(IPSec(initialize_sas :01:50:25
                           ,key Eng. msg.) dest= 19.19.19.19, src= 18.18.18.18)
                           ,(dest_proxy= 19.19.19.0/255.255.255.0/0/0 (type=4
                            ,(src_proxy= 18.18.18.0/255.255.255.0/0/0 (type=4
                                                  , protocol= AH, transform= ah-md5-hmac
                                                    ,lifedur= 3600s and 4608000kb
        spi= 0x176D0964(393021796), conn_id= 2000, keysize= 0, flags= 0x4
                                                  , :(IPSec(initialize_sas :01:50:25
                           ,key Eng. msg.) src= 19.19.19.19, dest= 18.18.18.18)
                            ,(src_proxy= 19.19.19.0/255.255.255.0/0/0 (type=4
                           ,(dest_proxy= 18.18.18.0/255.255.255.0/0/0 (type=4
                                                  , protocol= AH, transform= ah-md5-hmac
                                                    ,lifedur= 3600s and 4608000kb
        spi= 0x19911A16(428939798), conn_id= 2001, keysize= 0, flags= 0x4
                                                  , :(IPSec(initialize_sas :01:50:25
                           ,key Eng. msg.) dest= 19.19.19.19, src= 18.18.18.18)
```

```
,(dest_proxy= 19.19.19.0/255.255.255.0/0/0 (type=4
 ,(src_proxy= 18.18.18.0/255.255.255.0/0/0 (type=4
                    , protocol= ESP, transform= ESP-Des
                          ,lifedur= 3600s and 4608000kb
 spi= 0x2B92064(45686884), conn_id= 2002, keysize= 0, flags= 0x4
                         , :(IPSec(initialize_sas :01:50:25
,key Eng. msg.) src= 19.19.19.19, dest= 18.18.18.18)
 ,(src_proxy= 19.19.19.0/255.255.255.0/0/0 (type=4
,(dest_proxy= 18.18.18.0/255.255.255.0/0/0 (type=4
                    , protocol= ESP, transform= ESP-Des
                          ,lifedur= 3600s and 4608000kb
spi= 0x7091981(118036865), conn_id= 2003, keysize= 0, flags= 0x4
                      ,IPSec(create_sa): sa created :01:50:25
                   ,sa) sa_dest= 19.19.19.19, sa_prot= 51)
                          ,(sa_spi= 0x176D0964(393021796
                sa_trans= ah-md5-hmac , sa_conn_id= 2000
                     ,IPSec(create_sa): sa created :01:50:25
                   ,sa) sa_dest= 18.18.18.18, sa_prot= 51)
                          ,(sa_spi= 0x19911A16(428939798
                sa_trans= ah-md5-hmac , sa_conn_id= 2001
                     ,IPSec(create_sa): sa created :01:50:25
                   ,sa) sa_dest= 19.19.19.19, sa_prot= 50)
                           ,(sa_spi= 0x2B92064(45686884
                 sa_trans= ESP-Des , sa_conn_id= 2002
                  ,IPSec(create_sa): sa created :01:50:25
                ,sa) sa_dest= 18.18.18.18, sa_prot= 50)
                          ,(sa_spi= 0x7091981(118036865
                 sa_trans= ESP-Des , sa_conn_id= 2003
                                                ubr924-1#
```

بمجرد إنشاء نفق IPsec، يمكنك مشاهدة الاتصال والحزم المشفرة وغير المشفرة.

```
                                    ubr924-1#show crypto engine connection active
ID   Interface      IP-Address      State  Algorithm           Encrypt  Decrypt
set    HMAC_MD5+DES_56_CB       0        0                                 1
cable-modem0   172.16.31.20   set    HMAC_MD5                 0       99 2000
cable-modem0   172.16.31.20   set    HMAC_MD5                99        0 2001
cable-modem0   172.16.31.20   set    DES_56_CBC               0       99 2002
cable-modem0   172.16.31.20   set    DES_56_CBC              99        0 2003
```

يعرض السطر 200x الأول 99 حزمة مستلمة. عليه أن يفك تشفير الحزم in order to أرسلهم إلى PC1. يعرض السطر الثاني 99 حزمة مرسلة. يجب عليه تشفير الحزم قبل أن يرسلها إلى uBR904-2. ويقوم الأسطر الثالث والرابع بنفس العملية، ولكن مع تحويل ESP-DES بدلا من AH-MD5-HMAC.

ملاحظة: إذا كانت مجموعة التحويل التي تم تكوينها على مودم الكبل هي ESP-MD5-HMAC ESP-DES، فيمكنك مشاهدة نظامين مستقلين (ASs) فقط، مقارنة بالأنظمة الأربعة الموضحة في أمر **العرض السابق**.

```
                                    ubr904-2#show crypto engine connection active
ID   Interface      IP-Address      State  Algorithm           Encrypt  Decrypt
set    HMAC_MD5+DES_56_CB       0        0                                 1
cable-modem0   172.16.30.18   set    HMAC_MD5                 0       99 2000
cable-modem0   172.16.30.18   set    HMAC_MD5                99        0 2001
cable-modem0   172.16.30.18   set    DES_56_CBC               0       99 2002
cable-modem0   172.16.30.18   set    DES_56_CBC              99        0 2003
```

قم بإصدار إختبار اتصال موسع إلى PC2 من uBR924-1 لمعرفة ما إذا كانت العدادات تتزايد للحزم المشفرة وغير المشفرة.

```
ubr924-1#ping ip
Target IP address: 18.18.18.1
Repeat count [5]: 50
:[Datagram size [100
:[Timeout in seconds [2
Extended commands [n]: y
Source address or interface: 19.19.19.19
:[Type of service [0
:[Set DF bit in IP header? [no
:[Validate reply data? [no
:[Data pattern [0xABCD
:[Loose, Strict, Record, Timestamp, Verbose[none
:[Sweep range of sizes [n
.Type escape sequence to abort
:Sending 50, 100-byte ICMP Echos to 18.18.18.1, timeout is 2 seconds
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 28/30/33 ms

ubr924-1#show crypto engine connection active
ID   Interface       IP-Address      State  Algorithm          Encrypt  Decrypt
set    HMAC_MD5+DES_56_CB       0         0                            1
cable-modem0   172.16.31.20   set    HMAC_MD5                   0       149 2000
cable-modem0   172.16.31.20   set    HMAC_MD5                 149         0 2001
cable-modem0   172.16.31.20   set    DES_56_CBC                 0       149 2002
cable-modem0   172.16.31.20   set    DES_56_CBC               149         0 2003

ubr904-2#show crypto engine connection active
ID   Interface       IP-Address      State  Algorithm          Encrypt  Decrypt
set    HMAC_MD5+DES_56_CB       0         0                            1
cable-modem0   172.16.30.18   set    HMAC_MD5                   0       149 2000
cable-modem0   172.16.30.18   set    HMAC_MD5                 149         0 2001
cable-modem0   172.16.30.18   set    DES_56_CBC                 0       149 2002
cable-modem0   172.16.30.18   set    DES_56_CBC               149         0 2003
```

يمكن إصدار إختبار اتصال موسع آخر، لترى زيادة العدادات مرة أخرى. هذه المرة، قم بإرسال إختبار اتصال للحزم 500 من uBR904-2 إلى واجهة إيثرنت الخاصة ب 19.19.19.19) uBR924-1).

```
ubr904-2#ping ip
Target IP address: 19.19.19.19
Repeat count [5]: 500
Datagram size [100]: 1000
:[Timeout in seconds [2
Extended commands [n]: y
Source address or interface: 18.18.18.18
:[Type of service [0
:[Set DF bit in IP header? [no
:[Validate reply data? [no
:[Data pattern [0xABCD
:[Loose, Strict, Record, Timestamp, Verbose[none
:[Sweep range of sizes [n
.Type escape sequence to abort
:Sending 500, 1000-byte ICMP Echos to 19.19.19.19, timeout is 2 seconds
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
:IPSec(encapsulate): encaps area too small, moving to new buffer :01:59:06
!!!!!!!!!idbtype 0, encaps_size 26, header size 60, avail 84
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
!!!!!!!!!!
Success rate is 100 percent (500/500), round-trip min/avg/max = 98/135/352 ms

                                    ubr904-2#show crypto engine connection active
ID   Interface      IP-Address      State  Algorithm           Encrypt  Decrypt
set    HMAC_MD5+DES_56_CB       0        0                                 1
cable-modem0   172.16.30.18   set    HMAC_MD5                  0      649 2000
cable-modem0   172.16.30.18   set    HMAC_MD5                649        0 2001
cable-modem0   172.16.30.18   set    DES_56_CBC                0      649 2002
cable-modem0   172.16.30.18   set    DES_56_CBC              649        0 2003

                                    ubr924-1#show crypto engine connection active
ID   Interface      IP-Address      State  Algorithm           Encrypt  Decrypt
set    HMAC_MD5+DES_56_CB       0        0                                 1
cable-modem0   172.16.31.20   set    HMAC_MD5                  0      649 2000
cable-modem0   172.16.31.20   set    HMAC_MD5                649        0 2001
cable-modem0   172.16.31.20   set    DES_56_CBC                0      649 2002
cable-modem0   172.16.31.20   set    DES_56_CBC              649        0 2003
```

يمكنك إصدار أوامر **clear crypto isakmp** و**clear crypto sa** لمسح الاتصالات. أيضا، في حالة عدم وجود حركة مرور عبر نفق IPsec أثناء وقت انتهاء الصلاحية، يقوم IPsec بإعادة تعيين الاتصال تلقائيا.

استكشاف الأخطاء وإصلاحها

هناك حاليا ما من معلومة محددة يتوفر أن يتحرى هذا تشكيل.

معلومات ذات صلة

- أوامر أمان شبكة IPsec
- مقدمة عن تشفير أمان IPsec - معلومات تصحيح الأخطاء
- أمثلة تكوين IPsec
- تكوين أمان شبكة IPsec
- تكوين موجهات الوصول إلى الكبلات من السلسلة Cisco uBR900
- تنزيلات Cisco Cable/Broadband (**العملاء** المسجلون **فقط**)
- دعم تقنية كابل النطاق الترددي العريض
- 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).