تكوين مصادقة RADIUS و TACACS+ لعميل VPN باستخدام الموسعة

المحتويات

المقدمة

يوضح هذا المستند نموذجا لتكوينات مصادقة TACACS+ و RADIUS Internet Engineering Task Force (IETF)) الموسعة (Xauth). يتيح لك Xauth نشر أمان IP (IPSec) على الشبكات الخاصة الظاهرية (VPN) باستخدام TACACS+ أو RADIUS كطريقة مصادقة المستخدم الخاصة بك داخل بروتوكول تبادل مفتاح الإنترنت (IKE). توفر هذه الميزة مصادقة لمستخدم تم تثبيت CiscoSecure VPN Client 1.1 على الكمبيوتر الشخصي لديه، من خلال مطالبة المستخدم باسم مستخدم وكلمة مرور، ثم التحقق منهما باستخدام المعلومات المخزنة في خادم المصادقة والتخويل والمحاسبة (AAA) أو قاعدة بيانات TACACS+ أو RADIUS. تحدث المصادقة بين المرحلة 1 من IKE والمرحلة 2 من IKE. في حالة مصادقة المستخدم بنجاح، يتم إنشاء اقتران أمان للمرحلة 2 (SA) بعد ذلك يمكن إرسال البيانات بشكل آمن إلى الشبكة المحمية.

يتضمن Xauth *المصادقة* فقط، وليس *التفويض* (حيث يمكن للمستخدمين الانتقال بمجرد تأسيس الاتصال). لم يتم تنفيذ *المحاسبة* (حيث ذهب المستخدمون).

يجب أن يعمل التكوين بدون Xauth قبل تنفيذ Xauth. يوضح المثال الخاص بنا تكوين الوضع (mode config) وترجمة عنوان الشبكة (NAT) بالإضافة إلى Xauth، ولكن الافتراض هو أن اتصال IPSec موجود قبل إضافة أوامر Xauth.

تأكد من أن مصادقة (username/password) المحلية تعمل قبل محاولة TACACS+ أو RADIUS Xauth.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

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

- عميل شبكة VPN الإصدار 1.1 (أو إصدار أحدث)
- Cisco IOS® الإصدارات 12.1.2.2.P.12.1.2.2، T (أو الأحدث)
- تم إختبار مصادقة RADIUS مع Cisco 3640 التي تشغل c3640-jo3s56i-mz.121-2.3.T

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة 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.

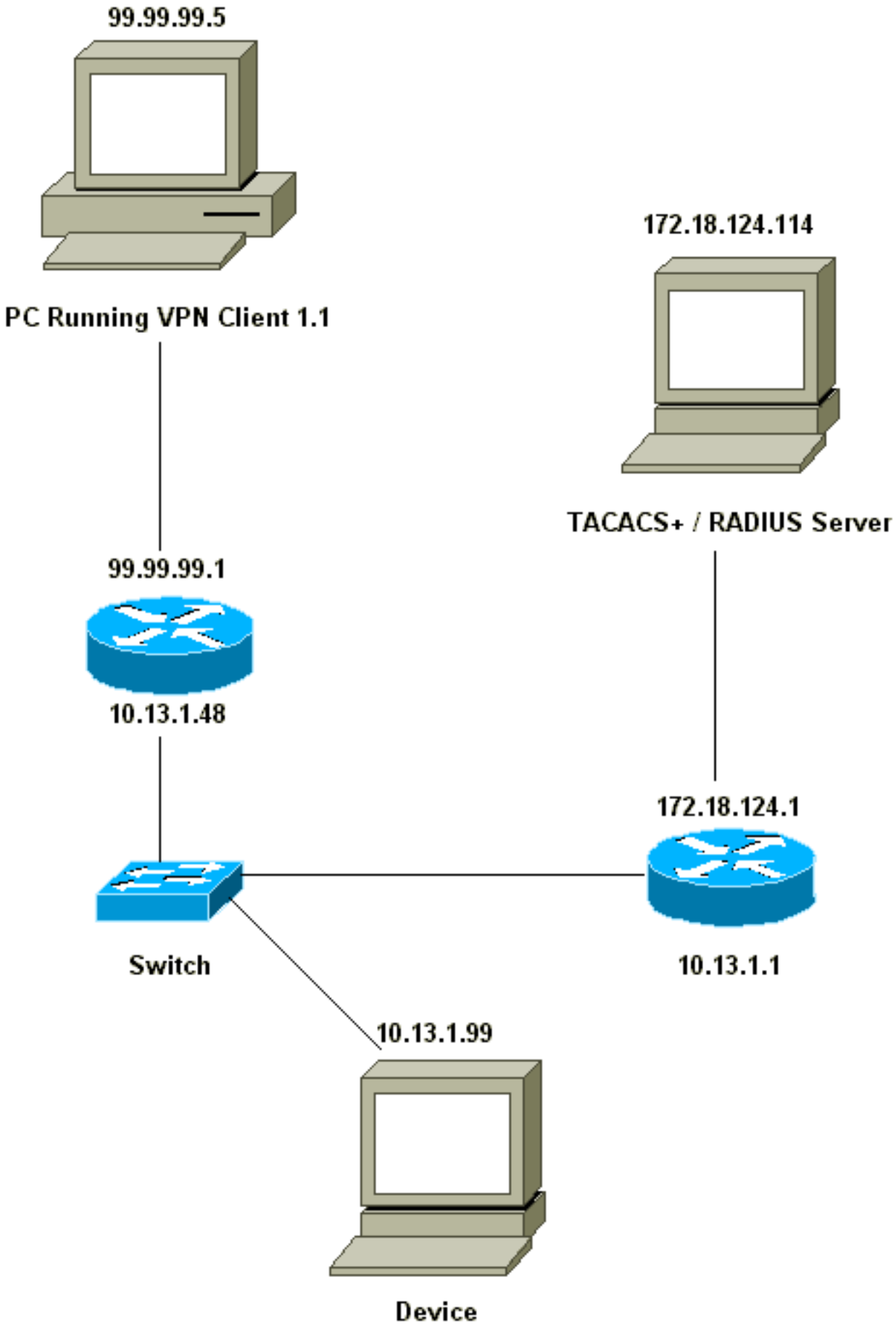
التكوين

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

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

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



إعداد عميل شبكة VPN 1.1

```
:Network Security policy
                                                    Myconn 1-
                                          My Identity = ip address
                                    Connection security: Secure
                              Remote Party Identity and addressing
                                       ID Type: IP subnet
                             (range of inside network) 10.13.1.0
                                    Port all Protocol all

                                      Connect using secure tunnel
                                      ID Type: IP address
                                               99.99.99.1
                                 Pre-shared key = cisco1234

                                                (Authentication (Phase 1
                                                        Proposal 1
                                 Authentication method: pre-shared key
                                                Encryp Alg: DES
                                                  Hash Alg: MD5
                                           SA life: Unspecified
                                                Key Group: DH 1

                                                 (Key exchange (Phase 2
                                                        Proposal 1
                                             Encapsulation ESP
                                              Encrypt Alg: DES
                                                 Hash Alg: MD5
                                                 Encap: tunnel
                                           SA life: Unspecified
                                                      no AH

                                                    Other Connections 2-
                                    Connection security: Non-secure
                                          Local Network Interface
                                                    Name: Any
                                                IP Addr: Any
                                                   Port: All
```

مع تمكين Xauth على الموجه، عندما يحاول المستخدم الاتصال بجهاز داخل الموجه (هنا قمنا ب ping -t #.#. #.#)، تظهر شاشة رمادية:

```
User Authentication for 3660
:Username
:Password
```

التكوينات

تكوين الخادم

يمكن إجراء مصادقة Xauth بواسطة TACACS+ أو بواسطة RADIUS. أردنا التأكد من أنه تم السماح لمستخدمي Xauth بتنفيذ Xauth، ولكن لم يتم السماح لهم باستخدام Telnet إلى الموجه، لذلك قمنا بإضافة أمر EXEC **لتفويض المصادقة والتفويض والمحاسبة (AAA)**. لقد أعطينا مستخدمي RADIUS "reply-attribute service-type=outbound=5" (بدلا من Administrative أو Login). في CiscoSecure UNIX، هذا هو "الصادر"؛ في CiscoSecure NT هذا هو "Dialout Framed." إذا كان هؤلاء مستخدمين ل TACACS+، فلن نعطيهم أذونات shell/exec.

تكوين موجه ل TACACS+ أو RADIUS Xauth
:Current configuration !

```
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname carter
!
Enable AAA and define authentication and ---!
authorization parameters aaa new-model
aaa authentication login default group radius|tacacs+
none
+aaa authentication login xauth_list group radius|tacacs
aaa authorization exec default group radius|tacacs+ none
enable secret 5 $1$VY18$uO2CRnqUzugV0NYtd14Gg0
enable password ww
!
username john password 0 doe
!
ip subnet-zero
ip audit notify log
ip audit po max-events 100
cns event-service server
!
crypto isakmp policy 10
hash md5
authentication pre-share
crypto isakmp key cisco1234 address 0.0.0.0 0.0.0.0
crypto isakmp client configuration address-pool local
ourpool
!
crypto ipsec transform-set mypolicy esp-des esp-md5-hmac
!
crypto dynamic-map dyna 10
set transform-set mypolicy
!
crypto map test client authentication list xauth_list
crypto map test client configuration address initiate
crypto map test client configuration address respond
crypto map test 5 ipsec-isakmp dynamic dyna
!
interface Ethernet0/0
ip address 10.13.1.48 255.255.255.0
ip nat inside
no ip route-cache
no ip mroute-cache
no mop enabled
!
interface TokenRing0/0
no ip address
shutdown
ring-speed 16
!
interface Ethernet2/0
ip address 99.99.99.1 255.255.255.0
ip nat outside
no ip route-cache
no ip mroute-cache
no mop enabled
crypto map test
!
interface TokenRing2/0
no ip address
shutdown
ring-speed 16
```

```
!
ip local pool ourpool 10.2.1.1 10.2.1.254
ip nat pool outsidepool 99.99.99.50 99.99.99.60 netmask
255.255.255.0
ip nat inside source route-map nonat pool outsidepool
ip classless
ip route 0.0.0.0 0.0.0.0 10.13.1.1
no ip http server
!
access-list 101 deny ip 10.13.1.0 0.0.0.255 10.2.1.0
0.0.0.255
access-list 101 permit ip 10.13.1.0 0.0.0.255 any
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
route-map nonat permit 10
match ip address 101
!
Define TACACS server host and key parameters ---!
tacacs-server host 172.18.124.114
tacacs-server key cisco
radius-server host 172.18.124.114 auth-port 1645 acct-
port 1646
radius-server retransmit 3
radius-server key cisco
!
line con 0
transport input none
line aux 0
line vty 0 4
password WW
!
end
```

التحقق من الصحة

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

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**.

- **debug aaa authentication**— يعرض معلومات حول مصادقة AAA/TACACS+.
- **debug crypto isakmp**—يعرض الرسائل المتعلقة بأحداث IKE.
- **debug crypto ipSec**—يعرض أحداث IPSec.
- **debug crypto key-exchange**—يعرض رسائل تبادل المفاتيح العامة لمعيار التوقيع الرقمي (DSS).
- **debug radius**—يعرض المعلومات المرتبطة ب RADIUS.
- **debug tacacs**— يعرض المعلومات المرتبطة ب tacacs.
- **مسح التشفير isakmp**—يحدد أي اتصال سيتم مسحه.

- **مسح التشفير sa**—يحذف اقترانات أمان IPSec.

إخراج تصحيح الأخطاء للعينة

ملاحظة: سيكون تصحيح أخطاء TACACS+ مماثلا جدا. أستخدم الأمر **debug tacacs+** بدلا من الأمر **debug radius**.

```
Carter#show debug
General OS:
  AAA Authentication debugging is on
  Radius protocol debugging is on
Cryptographic Subsystem:
  Crypto ISAKMP debugging is on
  Crypto Engine debugging is on
  Crypto IPSEC debugging is on
Carter#term mon
ISAKMP (0:0): received packet from 99.99.99.5 (N) NEW SA :03:12:54
ISAKMP: local port 500, remote port 500 :03:12:54
ISAKMP (0:1): Setting client config settings 6269C36C :03:12:54
ISAKMP (0:1): (Re)Setting client xauth list xauth_list :03:12:54
                                                and state
ISAKMP: Created a peer node for 99.99.99.5 :03:12:54
ISAKMP: Locking struct 6269C36C from :03:12:54
                          crypto_ikmp_config_initialize_sa
ISAKMP (0:1): processing SA payload. message ID = 0 :03:12:54
ISAKMP (0:1): found peer pre-shared key matching 99.99.99.5 :03:12:54
ISAKMP (0:1): Checking ISAKMP transform 1 against :03:12:54
                                        priority 10 policy
ISAKMP:      encryption DES-CBC :03:12:54
ISAKMP:      hash MD5 :03:12:54
ISAKMP:      default group 1 :03:12:54
ISAKMP:      auth pre-share :03:12:54
ISAKMP (0:1): atts are acceptable. Next payload is 0 :03:12:54
CryptoEngine0: generate alg parameter :03:12:54
CRYPTO_ENGINE: Dh phase 1 status: 0 :03:12:54
CRYPTO_ENGINE: DH phase 1 status: 0 :03:12:54
ISAKMP (0:1): SA is doing pre-shared key authentication using :03:12:54
                                        id type ID_IPV4_ADDR
ISAKMP (0:1): sending packet to 99.99.99.5 (R) MM_SA_SETUP :03:12:54
ISAKMP (0:1): received packet from 99.99.99.5 (R) MM_SA_SETUP :03:12:54
ISAKMP (0:1): processing KE payload. Message ID = 0 :03:12:54
CryptoEngine0: generate alg parameter :03:12:54
ISAKMP (0:1): processing NONCE payload. Message ID = 0 :03:12:54
ISAKMP (0:1): found peer pre-shared key matching 99.99.99.5 :03:12:54
CryptoEngine0: create ISAKMP SKEYID for conn id 1 :03:12:54
ISAKMP (0:1): SKEYID state generated :03:12:54
ISAKMP (0:1): processing vendor id payload :03:12:54
ISAKMP (0:1): processing vendor id payload :03:12:54
ISAKMP (0:1): sending packet to 99.99.99.5 (R) MM_KEY_EXCH :03:12:54
ISAKMP (0:1): received packet from 99.99.99.5 (R) MM_KEY_EXCH :03:12:55
ISAKMP (0:1): processing ID payload. Message ID = 0 :03:12:55
ISAKMP (0:1): processing HASH payload. Message ID = 0 :03:12:55
CryptoEngine0: generate hmac context for conn id 1 :03:12:55
ISAKMP (0:1): processing NOTIFY INITIAL_CONTACT protocol 1 :03:12:55
                                        spi 0, message ID = 0
ISAKMP (0:1): SA has been authenticated with 99.99.99.5 :03:12:55
ISAKMP (1): ID payload :03:12:55
        next-payload : 8
        type         : 1
      protocol     : 17
```

```
                                                port         : 500
                                                  length       : 8
                                ISAKMP (1): Total payload length: 12 :03:12:55
                    CryptoEngine0: generate hmac context for conn id 1 :03:12:55
                          CryptoEngine0: clear DH number for conn id 1 :03:12:55
       ISAKMP (0:1): sending packet to 99.99.99.5 (R) CONF_XAUTH :03:12:55
    ISAKMP (0:1): received packet from 99.99.99.5 (R) CONF_XAUTH :03:12:55
                       ISAKMP (0:1): (Re)Setting client xauth list :03:12:55
                                                  xauth_list and state
                                         ISAKMP (0:1): Need XAUTH :03:12:55
                           AAA: parse name=ISAKMP idb type=-1 tty=-1 :03:12:55
          ''=AAA/MEMORY: create_user (0x6269AD80) user='' ruser :03:12:55
                 port='ISAKMP' rem_addr='99.99.99.5' authen_type=ASCII
                                                  service=LOGIN priv=0
                       'AAA/AUTHEN/START (2289801324): port='ISAKMP :03:12:55
                             list='xauth_list' action=LOGIN service=LOGIN
           AAA/AUTHEN/START (2289801324): found list xauth_list :03:12:55
          (AAA/AUTHEN/START (2289801324): Method=radius (radius :03:12:55
                       AAA/AUTHEN (2289801324): status = GETUSER :03:12:55
                                       ISAKMP: got callback 1 :03:12:55
                         ISAKMP/xauth: request attribute XAUTH_TYPE :03:12:55
                      ISAKMP/xauth: request attribute XAUTH_MESSAGE :03:12:55
                     ISAKMP/xauth: request attribute XAUTH_USER_NAME :03:12:55
                ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD :03:12:55
                 CryptoEngine0: generate hmac context for conn id 1 :03:12:55
                .ISAKMP (0:1): initiating peer config to 99.99.99.5 :03:12:55
                                                        ID = -280774539
       ISAKMP (0:1): sending packet to 99.99.99.5 (R) CONF_XAUTH :03:12:55
                  ISAKMP (0:1): retransmitting phase 2 CONF_XAUTH :03:13:00
                                                        ... -280774539
                 :ISAKMP (0:1): incrementing error counter on sa :03:13:00
                                                      retransmit phase 2
                 :ISAKMP (0:1): incrementing error counter on sa :03:13:00
                                                      retransmit phase 2
      ISAKMP (0:1): retransmitting phase 2 -280774539 CONF_XAUTH :03:13:00
       ISAKMP (0:1): sending packet to 99.99.99.5 (R) CONF_XAUTH :03:13:00
    ISAKMP (0:1): received packet from 99.99.99.5 (R) CONF_XAUTH :03:13:02
               ISAKMP (0:1): processing transaction payload from :03:13:02
                                    Message ID = -280774539 .99.99.99.5
                CryptoEngine0: generate hmac context for conn id 1 :03:13:02
                                    ISAKMP: Config payload REPLY :03:13:02
                         ISAKMP/xauth: reply attribute XAUTH_TYPE :03:13:02
                    ISAKMP/xauth: reply attribute XAUTH_USER_NAME :03:13:02
                 ISAKMP/xauth: reply attribute XAUTH_USER_PASSWORD :03:13:02
    (''(AAA/AUTHEN/CONT (2289801324): continue_login (user='(undef :03:13:02
                       AAA/AUTHEN (2289801324): status = GETUSER :03:13:02
                  (AAA/AUTHEN (2289801324): Method=radius (radius :03:13:02
                       AAA/AUTHEN (2289801324): status = GETPASS :03:13:02
      ('AAA/AUTHEN/CONT (2289801324): continue_login (user='zeke :03:13:02
                       AAA/AUTHEN (2289801324): status = GETPASS :03:13:02
                  (AAA/AUTHEN (2289801324): Method=radius (radius :03:13:02
                                    RADIUS: ustruct sharecount=2 :03:13:02
      ,RADIUS: Initial Transmit ISAKMP id 29 172.18.124.114:1645 :03:13:02
                                                Access-Request, len 68
                                  Attribute 4 6 0A0D0130         :03:13:02
                                 Attribute 61 6 00000000         :03:13:02
                                  Attribute 1 6 7A656B65         :03:13:02
                                Attribute 31 12 39392E39         :03:13:02
                                 Attribute 2 18 D687A79D         :03:13:02
                 ,RADIUS: Received from id 29 172.18.124.114:1645 :03:13:02
                                                Access-Accept, Len 26
                                  Attribute 6 6 00000005         :03:13:02
               RADIUS: saved authorization data for user 6269AD80 :03:13:02
                                                          at 62634D0C
```

```
                                AAA/AUTHEN (2289801324): status = PASS :03:13:02
                                        ISAKMP: got callback 1 :03:13:02
                    CryptoEngine0: generate hmac context for conn id 1 :03:13:02
                   .ISAKMP (0:1): initiating peer config to 99.99.99.5 :03:13:02
                                                    ID = -280774539
              ISAKMP (0:1): sending packet to 99.99.99.5 (R) CONF_XAUTH :03:13:02
            ISAKMP (0:1): received packet from 99.99.99.5 (R) CONF_XAUTH :03:13:03
          .ISAKMP (0:1): processing transaction payload from 99.99.99.5 :03:13:03
                                                Message ID = -280774539
                    CryptoEngine0: generate hmac context for conn id 1 :03:13:03
                                        ISAKMP: Config payload ACK :03:13:03
                    ISAKMP (0:1): deleting node -280774539 error FALSE :03:13:03
                                        "reason "done with transaction
                              ISAKMP (0:1): allocating address 10.2.1.2 :03:13:03
                    CryptoEngine0: generate hmac context for conn id 1 :03:13:03
                   .ISAKMP (0:1): initiating peer config to 99.99.99.5 :03:13:03
                                                    ID = 2130856112
               ISAKMP (0:1): sending packet to 99.99.99.5 (R) CONF_ADDR :03:13:03
             ISAKMP (0:1): received packet from 99.99.99.5 (R) CONF_ADDR :03:13:03
                          ISAKMP (0:1): processing transaction payload :03:13:03
                                    from 99.99.99.5. Message ID = 2130856112
                    CryptoEngine0: generate hmac context for conn id 1 :03:13:03
                                        ISAKMP: Config payload ACK :03:13:03
                               !ISAKMP (0:1): peer accepted the address :03:13:03
                          ISAKMP (0:1): adding static route for 10.2.1.2 :03:13:03
               ISAKMP (0:1): installing route 10.2.1.2 255.255.255.255 :03:13:03
                                                            99.99.99.5
                    ISAKMP (0:1): deleting node 2130856112 error FALSE :03:13:03
                                        "reason "done with transaction
                         .ISAKMP (0:1): Delaying response to QM request :03:13:03
             ISAKMP (0:1): received packet from 99.99.99.5 (R) QM_IDLE :03:13:04
                ISAKMP (0:1): (Re)Setting client xauth list xauth_list :03:13:04
                                                              and state
                    CryptoEngine0: generate hmac context for conn id 1 :03:13:04
        ISAKMP (0:1): processing HASH payload. Message ID = -1651205463 :03:13:04
          ISAKMP (0:1): processing SA payload. Message ID = -1651205463 :03:13:04
                               ISAKMP (0:1): Checking IPSec proposal 1 :03:13:04
                                        ISAKMP: transform 1, ESP_DES :03:13:04
                                   :ISAKMP:   attributes in transform :03:13:04
                                ISAKMP:      authenticator is HMAC-MD5 :03:13:04
                                     ISAKMP:      encaps is 1 :03:13:04
                                          validate proposal 0 :03:13:04
                                   .ISAKMP (0:1): atts are acceptable :03:13:04
                   ,IPSEC(validate_proposal_request): proposal part #1 :03:13:04
                            ,key eng. msg.) dest= 99.99.99.1, src= 99.99.99.5)
                           ,(dest_proxy= 10.13.1.0/255.255.255.0/0/0 (type=4
                           ,(src_proxy= 10.2.1.2/255.255.255.255/0/0 (type=1
                            , protocol= ESP, transform= ESP-Des esp-md5-hmac
                                                    ,lifedur= 0s and 0kb
                             spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
                                        validate proposal request 0 :03:13:04
                               .ISAKMP (0:1): processing NONCE payload :03:13:04
                                                Message ID = -1651205463
                                  .ISAKMP (0:1): processing ID payload :03:13:04
                                                Message ID = -1651205463
                       ISAKMP (1): ID_IPV4_ADDR src 10.2.1.2 prot 0 port 0 :03:13:04
                                  .ISAKMP (0:1): processing ID payload :03:13:04
                                                Message ID = -1651205463
          ISAKMP (1): ID_IPV4_ADDR_SUBNET dst 10.13.1.0/255.255.255.0 :03:13:04
                                                          port 0 port 0
                           ISAKMP (0:1): asking for 1 spis from ipsec :03:13:04
                              ...IPSEC(key_engine): got a queue event :03:13:04
                         IPSEC(spi_response): getting spi 570798685 for SA :03:13:04
                          from 99.99.99.5      to 99.99.99.1      for prot 3
```

```
(ISAKMP: received ke message (2/1 :03:13:04
CryptoEngine0: generate hmac context for conn id 1 :03:13:04
ISAKMP (0:1): sending packet to 99.99.99.5 (R) QM_IDLE :03:13:04
ISAKMP (0:1): received packet from 99.99.99.5 (R) QM_IDLE :03:13:04
CryptoEngine0: generate hmac context for conn id 1 :03:13:04
ipsec allocate flow 0 :03:13:04
ipsec allocate flow 0 :03:13:04
ISAKMP (0:1): Creating IPSec SAs :03:13:04
inbound SA from 99.99.99.5 to 99.99.99.1 :03:13:04
(proxy 10.2.1.2 to 10.13.1.0)
has spi 0x2205B25D and conn_id 2000 and flags 4 :03:13:04
outbound SA from 99.99.99.1 to 99.99.99.5 :03:13:04
(proxy 10.13.1.0 to 10.2.1.2)
has spi -1338747879 and conn_id 2001 and flags 4 :03:13:04
ISAKMP (0:1): deleting node -195511155 error FALSE :03:13:04
"reason "saved qm no longer needed
ISAKMP (0:1): deleting node -1651205463 error FALSE :03:13:04
"()reason "quick mode done (await
...IPSEC(key_engine): got a queue event :03:13:04
, :(IPSEC(initialize_sas :03:13:04
,key eng. msg.) dest= 99.99.99.1, src= 99.99.99.5)
,(dest_proxy= 10.13.1.0/255.255.255.0/0/0 (type=4
,(src_proxy= 10.2.1.2/0.0.0.0/0/0 (type=1
, protocol= ESP, transform= esp-des esp-md5-hmac
,lifedur= 0s and 0kb
,spi= 0x2205B25D(570798685), conn_id= 2000
keysize= 0, flags= 0x4
, :(IPSEC(initialize_sas :03:13:04
,key eng. msg.) src= 99.99.99.1, dest= 99.99.99.5)
,(src_proxy= 10.13.1.0/255.255.255.0/0/0 (type=4
,(dest_proxy= 10.2.1.2/0.0.0.0/0/0 (type=1
, protocol= ESP, transform= esp-des esp-md5-hmac
,lifedur= 0s and 0kb
,spi= 0xB0345419(2956219417), conn_id= 2001
keysize= 0, flags= 0x4
,IPSEC(create_sa): sa created :03:13:04
,sa) sa_dest= 99.99.99.1, sa_prot= 50)
,(sa_spi= 0x2205B25D(570798685
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2000
,IPSEC(create_sa): sa created :03:13:04
,sa) sa_dest= 99.99.99.5, sa_prot= 50)
,(sa_spi= 0xB0345419(2956219417
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2001
(ISAKMP: received ke message (4/1 :03:13:04
ISAKMP: Locking struct 6269C36C for IPSEC :03:13:04
IPSEC(decapsulate): error in decapsulation :03:13:05
crypto_ipsec_sa_exists
```

معلومات ذات صلة

- صفحة دعم عميل شبكة VPN من Cisco
- صفحة دعم مفاوضة IPSec/بروتوكولات IKE
- صفحة دعم نظام مراقبة الدخول إلى وحدة تحكم الوصول إلى المحطة الطرفية (TACACS+)
- صفحة دعم خدمة مصادقة طلب اتصال المستخدم البعيد (RADIUS)
- طلب التعليقات
- 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).