VPN クライアントを使用する TACACS+ および RADIUS拡張認証の設定

内容

概要
前提条件
要件
使用するコンポーネント
表記法
設定
ネットワーク図
VPN Client 1.1の設定
設定
確認
トラブルシュート
トラブルシューティングのためのコマンド
debug 出力例
関連情報

概要

このドキュメントでは、TACACS+ および RADIUS インターネット技術特別調査委員会（IETF）拡張認証（Xauth）の設定例を説明します。 Xauthを使用すると、TACACS+またはRADIUSをインターネットキーエクスチェンジ(IKE)プロトコル内のユーザ認証方式として使用して、仮想プライベートネットワーク(VPN)にIPセキュリティ(IPSec)を導入できます。この機能は、PCにCiscoSecure VPN Client 1.1がインストールされているユーザに認証を提供します。ユーザ名とパスワードを入力し、認証、許可、アカウンティング(AAA)サーバ、TACACS+またはRADIUSデータベースに保存されている情報で検証します。認証はIKEフェーズ1とIKEフェーズ2の間で行われます。ユーザが正常に認証されると、フェーズ2セキュリティアソシエーション(SA)が確立され、その後でデータが保護されたネットワークに安全に送信されます。

Xauthには認証*のみが含まれ*、認証は含*まれません*（ユーザは接続が確立された後にアクセスできます）。 *アカウンティング*（ユーザが行った場所）は実装されていません。

Xauthを実装する前に、Xauthなしで設定が機能する必要があります。この例では、Xauthに加えてMode Configuration(Mode Config)とNetwork Address Translation(NAT)を示していますが、Xauthコマンドを追加する前にIPSec接続が存在することを前提としています。

TACACS+またはRADIUS Xauthを試行する前に、ローカルXauth（ルータのユーザ名/パスワード）が動作することを確認します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- VPN Clientバージョン1.1（またはそれ以降）
- Cisco IOS® リリース12.1.2.2.T、12.1.2.2.P（以降）
- RADIUS認証は、c3640-jo3s56i-mz.121-2.3.Tを実行するCisco 3640でテストされました

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

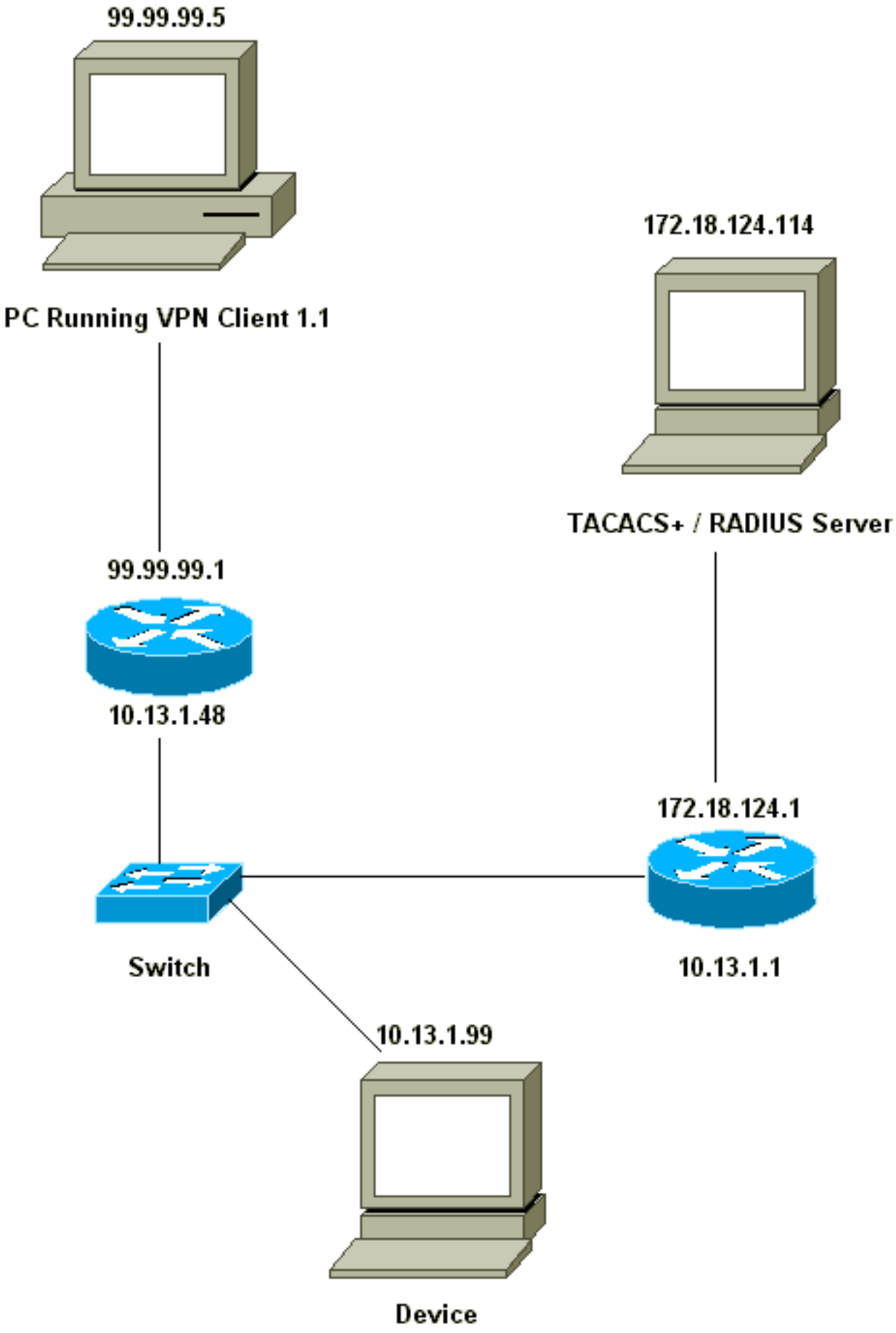
設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注：このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことをご了承ください。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



[VPN Client 1.1の設定]

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

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

ルータでXauthを有効にすると、ユーザがルータ内部のデバイスに接続しようとすると（ここではping -t #.#.#.#を実行しました）、灰色の画面が表示されます。

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

設定

サーバの設定

Xauth認証は、TACACS+またはRADIUSのいずれかで実行できます。XauthユーザはXauthを実行できますが、ルータへのTelnetは許可されていないことを確認するため、**aaa authorization execコマンドを追加し**ました。RADIUSユーザに対して、（AdministrativeまたはLoginではなく）reply-attribute Service-Type=Outbound=5」と入力しました。 CiscoSecure UNIXでは、「アウトバウンド」です。CiscoSecure NTでは「Dialout Framed」です。 これらがTACACS+ユーザである場合、シェル/exec権限は付与されません。

TACACS+またはRADIUS Xauthのルータ設定
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
```

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

トラブルシューティングのためのコマンド

アウトプット インタープリタ ツール（登録ユーザ専用）（OIT）は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

注：debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

- **debug aaa authentication**：AAA/TACACS+ 認証に関する情報を表示します。
- **debug crypto isakmp**：IKE イベントに関するメッセージを表示します。
- **debug crypto ipsec**：IPsec イベントを表示します。
- **debug crypto key-exchange**:Digital Signature Standard（DSS；デジタル署名基準）公開鍵交換メッセージを表示します。
- **debug radius**:RADIUSに関連する情報を表示します。
- **debug tacacs**:TACACSに関連する情報を表示します。

- **clear crypto isakmp**：クリアする接続を指定します。
- **clear crypto sa**:IPSecセキュリティアソシエーションを削除します。

debug 出力例

注：TACACS+のデバッグは非常によく似ています。debug radiusコマンドの代**わりに、debug tacacs+**コマンドを使用**してください**。

```
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
03:12:54: 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
   and state
03:12:54: ISAKMP: Created a peer node for 99.99.99.5
03:12:54: ISAKMP: Locking struct 6269C36C from
   crypto_ikmp_config_initialize_sa
03:12:54: 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
   priority 10 policy
03:12:54: 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
   id type ID_IPV4_ADDR
03:12:54: 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
03:12:55: 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
        spi 0, message ID = 0
03:12:55: ISAKMP (0:1): SA has been authenticated with 99.99.99.5
03:12:55: ISAKMP (1): ID payload
        next-payload : 8
        type         : 1
```

```
        protocol     : 17
        port         : 500
        length       : 8
03:12:55: 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
   xauth_list and state
03:12:55: 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=''
   port='ISAKMP' rem_addr='99.99.99.5' authen_type=ASCII
   service=LOGIN priv=0
03:12:55: AAA/AUTHEN/START (2289801324): port='ISAKMP'
   list='xauth_list' action=LOGIN service=LOGIN
03:12:55: 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.
   ID = -280774539
03:12:55: ISAKMP (0:1): sending packet to 99.99.99.5 (R) CONF_XAUTH
03:13:00: ISAKMP (0:1): retransmitting phase 2 CONF_XAUTH
    -280774539 ...
03:13:00: ISAKMP (0:1): incrementing error counter on sa:
   retransmit phase 2
03:13:00: ISAKMP (0:1): incrementing error counter on sa:
   retransmit phase 2
03:13:00: 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
03:13:02: ISAKMP (0:1): received packet from 99.99.99.5 (R) CONF_XAUTH
03:13:02: ISAKMP (0:1): processing transaction payload from
   99.99.99.5. Message ID = -280774539
03:13:02: 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,
   Access-Request, len 68
03:13:02:         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,
   Access-Accept, Len 26
03:13:02:         Attribute 6 6 00000005
03:13:02: RADIUS: saved authorization data for user 6269AD80
```

```
   at 62634D0C
03:13:02: 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.
   ID = -280774539
03:13:02: ISAKMP (0:1): sending packet to 99.99.99.5 (R) CONF_XAUTH
03:13:03: 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.
   Message ID = -280774539
03:13:03: 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
   reason "done with transaction"
03:13:03: 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.
   ID = 2130856112
03:13:03: 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
   from 99.99.99.5. Message ID = 2130856112
03:13:03: 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
   99.99.99.5
03:13:03: ISAKMP (0:1): deleting node 2130856112 error FALSE
   reason "done with transaction"
03:13:03: ISAKMP (0:1): Delaying response to QM request.
03:13:04: 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
   and state
03:13:04: 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,
  (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
03:13:04: validate proposal request 0
03:13:04: ISAKMP (0:1): processing NONCE payload.
   Message ID = -1651205463
03:13:04: ISAKMP (0:1): processing ID payload.
   Message ID = -1651205463
03:13:04: ISAKMP (1): ID_IPV4_ADDR src 10.2.1.2 prot 0 port 0
03:13:04: ISAKMP (0:1): processing ID payload.
   Message ID = -1651205463
03:13:04: ISAKMP (1): ID_IPV4_ADDR_SUBNET dst 10.13.1.0/255.255.255.0
   port 0 port 0
03:13:04: 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
```

```
        from 99.99.99.5      to 99.99.99.1      for prot 3
03:13:04: 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
        (proxy 10.2.1.2 to 10.13.1.0)
03:13:04:         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
   (proxy 10.13.1.0 to 10.2.1.2)
03:13:04:         has spi -1338747879 and conn_id 2001 and flags 4
03:13:04: ISAKMP (0:1): deleting node -195511155 error FALSE
   reason "saved qm no longer needed"
03:13:04: ISAKMP (0:1): deleting node -1651205463 error FALSE
   reason "quick mode done (await()"
03:13:04: IPSEC(key_engine): got a queue event...
03:13:04: IPSEC(initialize_sas): ,
  (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
03:13:04: IPSEC(initialize_sas): ,
  (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
03:13:04: IPSEC(create_sa): sa created,
  (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
03:13:04: IPSEC(create_sa): sa created,
  (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
03:13:04: ISAKMP: received ke message (4/1)
03:13:04: ISAKMP: Locking struct 6269C36C for IPSEC
03:13:05: IPSEC(decapsulate): error in decapsulation
   crypto_ipsec_sa_exists
```

関連情報

- Cisco VPN Client に関するサポート ページ
- IPSec ネゴシエーション/IKE プロトコルに関するサポート ページ
- Terminal Access Controller Access Control System (TACACS+) に関するサポート ページ
- Remote Authentication Dial-In User Service (RADIUS) に関するサポート ページ
- Request for Comments
- テクニカル サポートとドキュメント – Cisco Systems