

ハブ PIX とリモート PIX 間における、VPN Client と拡張認証を使用した IPSec 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](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

[トラブルシューティングのためのコマンド](#)

[ハブ PIX からのデバッグ](#)

[関連情報](#)

概要

このドキュメントでは、ゲートウェイ間およびリモート ユーザ機能に関する IPSec の設定を説明します。Extended Authentication (Xauth; 拡張認証) を使用すると、デバイスは事前共有鍵によって認証され、ユーザはユーザ名とパスワードの確認要求によって認証されます。

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。

- PIX Firewallバージョン6.3(3)
- Cisco VPN Client バージョン 3.5
- Cisco Secure ACS for Windows バージョン 2.6

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。

背景説明

この例では、リモート PIX からハブ PIX へのゲートウェイ間 IPsec トンネルがあります。このトンネルにより、リモート PIX の背後にあるネットワーク 10.48.67.x から、ハブ PIX の背後にあるネットワーク 10.48.66.x へのトラフィックが暗号化されます。インターネット上の PC は、ハブ PIX を介してネットワーク 10.48.66.x への IPsec トンネルを形成できます。

Xauth 機能を使用するには、まず基本的な認証、許可、アカウントिंग(AAA)サーバを設定する必要があります。crypto map client authentication コマンドを使用して、IKE (インターネットキーエクスチェンジ) のフェーズ 1 で Xauth (RADIUS/TACACS+ ユーザ名とパスワード) チャレンジを使用するように PIX ファイアウォールに指示します。Xauth が失敗すると、IKE セキュリティアソシエーションは確立されません。aaa-server コマンド文で指定した crypto map client authentication コマンド文書内で、同じ AAA サーバ名を指定してください。リモートユーザは、Cisco VPN Client バージョン 3.x を実行する必要があります。またはそれ以降

注：Cisco VPN Client 3.5.x 以降を使用することをお勧めします。VPN Client 1.1 はこの設定では動作しないため、このドキュメントの範囲外です。

注：Cisco VPN Client 3.6 以降では、des/sha のトランスフォームセットはサポートされていません。

Xauth を使用しない設定を復元する必要がある場合、no crypto map client authentication コマンドを使用します。デフォルトでは、Xauth 機能は有効になっていません。

注：暗号化テクノロジーは、輸出規制の対象となります。暗号化技術の輸出に関する法律を知るのは、お客様の責任です。詳細は、[輸出管理局のホームページを参照してください](#)。輸出規制に関するご質問がございましたら、export@cisco.com まで電子メールでお問い合わせください。

注：PIX Firewall バージョン 5.3 以降、設定可能な RADIUS ポートが導入されました。一部の RADIUS サーバは、1645/1646 以外の RADIUS ポート (通常は 1812/1813) を使用します。PIX 5.3 以降では、次のコマンドを使用して、RADIUS 認証およびアカウントिंगポートをデフォルトの 1645/1646 以外のポートに変更できます。

```
aaa-server radius-authport #  
aaa-server radius-acctport #
```

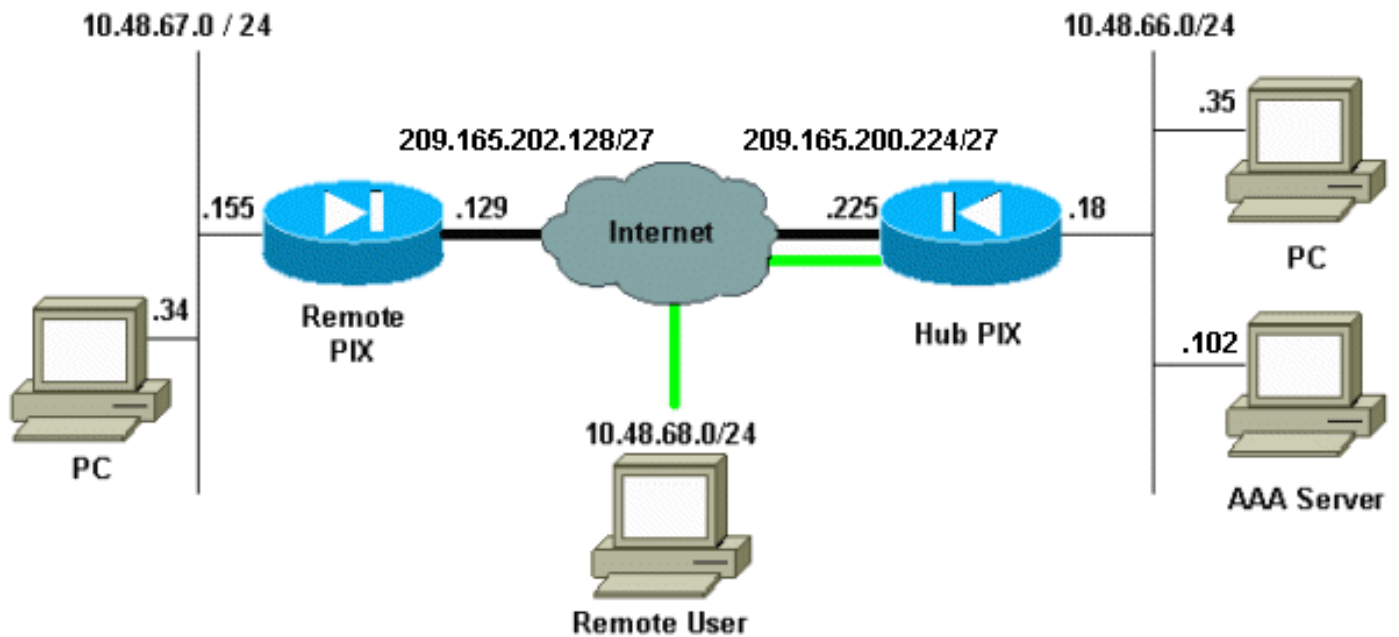
設定

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：このドキュメント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](#)) を使用してください。

ネットワーク図

この図では、VPNトンネルを示すために緑色と黒色の太字の線を使用しています。



設定

このドキュメントでは次の設定を使用します。

- [ハブPIX](#)
- [リモートPIX](#)

注：このドキュメントの例では、VPNサーバのIPアドレスは209.165.200.225、グループ名は「vpn3000」、グループパスワードは「cisco」です。

ハブ PIX のコンフィギュレーション

```
PIX Version 6.3(3)
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password OnTrBUG1Tp0edmkr encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname hubfixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
!--- Include traffic in the encryption process. access-
list 101 permit ip 10.48.66.0 255.255.255.0 10.48.67.0
```

```
255.255.255.0
!--- Accept traffic from the Network Address Translation
(NAT) process
access-list nonat permit ip 10.48.66.0 255.255.255.0
10.48.67.0 255.255.255.0
access-list nonat permit ip 10.48.66.0 255.255.255.0
10.48.68.0 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
ip address outside 209.165.200.225 255.255.255.224
ip address inside 10.48.66.18 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
ip local pool mypool 10.48.68.1-10.48.68.254
no failover
failover timeout 0:00:00
failover poll 15
no failover ip address outside
no failover ip address inside
pdm history enable
arp timeout 14400
global (outside) 1 209.16.200.230-209.16.200.240 netmask
255.255.255.224
global (outside) 1 209.16.200.241
!--- Except traffic from the NAT process. nat (inside) 0
access-list nonat
nat (inside) 1 10.48.66.0 255.255.255.0 0 0
route outside 0.0.0.0 0.0.0.0 209.165.200.226 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media
0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
aaa-server mytacacs protocol tacacs+
aaa-server mytacacs (inside) host 10.48.66.102 cisco
timeout 5
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
crypto ipsec transform-set myset esp-des esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set myset
!--- Use the crypto-map sequence 10 command for PIX to
PIX.

crypto map mymap 10 ipsec-isakmp
crypto map mymap 10 match address 101
crypto map mymap 10 set peer 209.165.202.129
crypto map mymap 10 set transform-set myset
!--- Use the crypto-map sequence 20 command for PIX to
VPN Client.

crypto map mymap 20 ipsec-isakmp dynamic dynmap
crypto map mymap client authentication mytacacs
crypto map mymap interface outside
isakmp enable outside
isakmp key ***** address 209.165.202.129 netmask
```

```
255.255.255.255
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5
!--- ISAKMP policy for VPN Client that runs 3.x code
needs to be DH group 2. isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
!--- IPsec group configuration for VPN Client. vpngroup
vpn3000 address-pool mypool
vpngroup vpn3000 dns-server 10.48.66.129
vpngroup vpn3000 wins-server 10.48.66.129
vpngroup vpn3000 default-domain cisco.com
vpngroup vpn3000 idle-time 1800
vpngroup vpn3000 password *****
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:7293dd9fc7c58ff5d65f042dd6ddbe13
: end
```

リモート PIX のコンフィギュレーション

```
PIX Version 6.3(3)
interface ethernet0 auto
interface ethernet1 100basex
interface ethernet2 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security4
enable password OnTrBUG1Tp0edmkr encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname remote
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
access-list 101 permit ip 10.48.67.0 255.255.255.0
10.48.66.0 255.255.255.0
!--- Accept traffic from the NAT process. access-list
nonat permit ip 10.48.67.0 255.255.255.0 10.48.66.0
255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
mtu intf2 1500
ip address outside 209.165.202.129 255.255.255.224
ip address inside 10.48.67.155 255.255.255.0
no ip address intf2
ip audit info action alarm
ip audit attack action alarm
no failover
```

```
failover timeout 0:00:00
failover poll 15
no failover ip address outside
no failover ip address inside
no failover ip address intf2
pdm history enable
arp timeout 14400
global (outside) 1 209.16.202.135-209.16.202.145 netmask
255.255.255.224
global (outside) 1 209.16.202.146
!--- Except traffic from the NAT process. nat (inside) 0
access-list nonat
nat (inside) 1 10.48.0.0 255.255.255.0 0 0
nat (inside) 1 10.48.67.0 255.255.255.0 0 0
route outside 0.0.0.0 0.0.0.0 209.165.202.130 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media
0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
crypto ipsec transform-set myset esp-des esp-md5-hmac
crypto map mymap 10 ipsec-isakmp
!--- Include traffic in the encryption process. crypto
map mymap 10 match address 101
crypto map mymap 10 set peer 209.165.200.225
crypto map mymap 10 set transform-set myset
crypto map mymap interface outside
isakmp enable outside
isakmp key ***** address 209.165.200.225 netmask
255.255.255.255
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:13ef4d29384c65c2cd968b5d9396f6e8
: end
```

VPN Clientの設定方法の詳細については、『[PIXからPIXおよびVPN Client 3.xへのPIXの設定](#)』の「設定」セクションを参照してください。また、PIX IPsecへのAAA認証の設定の詳細については、『[PIX IPsec 5.2以降へのAAA認証\(Xauth\)の追加方法](#)』を参照してください。

確認

このセクションでは、設定が正しく動作していることを確認するために使用できる情報を提供しています。

[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。

- show crypto isakmp sa : フェーズ 1 のセキュリティ アソシエーションを表示します。
- show crypto ipsec sa : フェーズ 2 のセキュリティ結合を表示します。

[トラブルシューティング](#)

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。

これらのデバッグは、両方の IPsec ルータ (ピア) で実行する必要があります。セキュリティ結合は両方のピアでクリアする必要があります。

- debug crypto isakmp : フェーズ 1 のエラーを表示します。
- debug crypto ipsec : フェーズ 2 のエラーを表示します。
- debug crypto engine : 暗号エンジンからの情報を表示します。
- clear crypto isakmp sa : フェーズ 1 のセキュリティアソシエーションをクリアします。
- clear crypto ipsec sa : フェーズ 2 のセキュリティアソシエーションをクリアします。
- debug radius [session | all | user username]:PIX 6.2 で使用できます。このコマンドは、RADIUS セッション情報と、送受信された RADIUS パケットの属性をログに記録します。
- debug tacacs [session|user <user_name>]:PIX 6.3 で使用可能です。このコマンドは TACACS 情報をログに記録します。
- debug aaa [authentication|authorization|accounting|internal]:PIX 6.3 で使用可能な AAA サブシステム情報が表示されます。

[ハブ PIX からのデバッグ](#)

注 : IPsec ネゴシエーションが成功した場合は、Cisco Bug ID [CSCdu84168 \(登録ユーザ専用\)](#) (内部 Cisco Bug ID [CSCdt31745](#)) が原因で、[すべてのデバッグが PIX で表示表示されない点があることに注意してください\(登録ユーザ専用\)](#)。このドキュメントの執筆時点では、この問題はまだ解決されていません。

注 : VPN Client からの IPsec VPN が PIX で終端しないことがあります。この問題を解決するには、クライアント PC にファイアウォールがないことを確認します。ファイアウォールが存在する場合は、UDP ポート 500 および 4500 が無効になっているかどうかを確認します。このような場合は、IPsec over TCP を有効にするか、UDP ポートのブロックを解除します。

[ハブおよびリモートの PIX 間のダイナミック IPsec トンネルのデバッグ](#)

```
crypto_isakmp_process_block:src:209.165.202.129,  
dest:209.165.200.225 spt:500 dpt:500
```

OAK_MM exchange
ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy
ISAKMP: encryption DES-CBC
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80
ISAKMP (0): **atts are acceptable**. Next payload is 0
ISAKMP (0): SA is doing pre-shared key authentication using id type ID_IPV4_ADDR
return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:209.165.202.129, dest:209.165.200.225
spt:500 dpt:500

OAK_MM exchange
ISAKMP (0): processing KE payload. message ID = 0

ISAKMP (0): processing NONCE payload. message ID = 0

ISAKMP (0): processing vendor id payload

ISAKMP (0): received xauth v6 vendor id

ISAKMP (0): processing vendor id payload

ISAKMP (0): remote peer supports dead peer detection

ISAKMP (0): processing vendor id payload

ISAKMP (0): processing vendor id payload

ISAKMP (0): speaking to another IOS box!

return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:209.165.202.129, dest:209.165.200.225
spt:500 dpt:500

OAK_MM exchange
ISAKMP (0): processing ID payload. message ID = 0
ISAKMP (0): processing HASH payload. message ID = 0
ISAKMP (0): SA has been authenticated

ISAKMP: Created a peer struct for 209.165.202.129, peer port 62465
ISAKMP (0): ID payload
next-payload : 8
type : 1
protocol : 17
port : 500
length : 8

ISAKMP (0): Total payload length: 12
return status is IKMP_NO_ERROR
ISAKMP (0): sending INITIAL_CONTACT notify
ISAKMP (0): sending NOTIFY message 24578 protocol 1
VPN Peer: ISAKMP: **Added new peer**: ip:209.165.202.129/500 Total VPN Peers:1
VPN Peer: ISAKMP: Peer ip:209.165.202.129/500 Ref cnt incremented to:1
Total VPN Peers:1
crypto_isakmp_process_block:src:209.165.202.129, dest:209.165.200.225
spt:500 dpt:500
ISAKMP (0): processing NOTIFY payload 24578 protocol 1
spi 0, message ID = 863921625
ISAKMP (0): processing notify INITIAL_CONTACTIPSEC(key_engine):
got a queue event...
IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
IPSEC(key_engine_delete_sas): delete all SAs shared with 209.165.202.129


```
return status is IKMP_NO_ERR_NO_TRANS
crypto_isakmp_process_block:src:209.165.202.129, dest:209.165.200.225
spt:500 dpt:500
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 2542705093

ISAKMP : Checking IPsec proposal 1

ISAKMP: transform 1, ESP_DES
ISAKMP:  attributes in transform:
ISAKMP:  encaps is 1
ISAKMP:  SA life type in seconds
ISAKMP:  SA life duration (basic) of 28800
ISAKMP:  SA life type in kilobytes
ISAKMP:  SA life duration (VPI) of  0x0 0x46 0x50 0x0
ISAKMP:  authenticator is HMAC-MD5
ISAKMP (0): atts are acceptable.IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) dest= 209.165.200.225, src= 209.165.202.129,
  dest_proxy= 10.48.66.0/255.255.255.0/0/0 (type=4),
  src_proxy= 10.48.67.0/255.255.255.0/0/0 (type=4),
  protocol= ESP, transform= esp-des esp-md5-hmac ,
  lifedur= 0s and 0kb,
  spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4

ISAKMP (0): processing NONCE payload. message ID = 2542705093

ISAKMP (0): processing ID payload. message ID = 2542705093
ISAKMP (0): ID_IPV4_ADDR_SUBNET src 10.48.67.0/255.255.255.0 prot 0 port 0
ISAKMP (0): processing ID payload. message ID = 2542705093
ISAKMP (0): ID_IPV4_ADDR_SUBNET dst 10.48.66.0/255.255.255.0 prot 0 port 0
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0x858c841a(2240578586) for SA
  from 209.165.202.129 to 209.165.200.225 for prot 3

return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:209.165.202.129, dest:209.165.200.225
spt:500 dpt:500
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAIT
ISAKMP (0): Creating IPsec SAs
  inbound SA from 209.165.202.129 to 209.165.200.225
    (proxy 10.48.67.0 to 10.48.66.0)
    has spi 2240578586 and conn_id 3 and flags 4
    lifetime of 28800 seconds
    lifetime of 4608000 kilobytes
  outbound SA from 209.165.200.225 to 209.165.202.129
    (proxy 10.48.66.0 to 10.48.67.0)
    has spi 681010504 and conn_id 4 and flags 4
    lifetime of 28800 seconds
    lifetime of 4608000 kilobytes
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
(key eng. msg.) dest= 209.165.200.225, src= 209.165.202.129,
  dest_proxy= 10.48.66.0/255.255.255.0/0/0 (type=4),
  src_proxy= 10.48.67.0/255.255.255.0/0/0 (type=4),
  protocol= ESP, transform= esp-des esp-md5-hmac ,
  lifedur= 28800s and 4608000kb,
  spi= 0x858c841a(2240578586), conn_id= 3, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
(key eng. msg.) src= 209.165.200.225, dest= 209.165.202.129,
  src_proxy= 10.48.66.0/255.255.255.0/0/0 (type=4),
```

```
dest_proxy= 10.48.67.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 28800s and 4608000kb,
spi= 0x28976548(681010504), conn_id= 4, keysize= 0, flags= 0x4
```

VPN Peer: IPSEC: Peer ip:209.165.202.129/500

Ref cnt incremented to:2 Total VPN Peers:1

VPN Peer: IPSEC: Peer ip:209.165.202.129/500

Ref cnt incremented to:3 Total VPN Peers:1

return status is IKMP_NO_ERROR

[VPN ClientをハブPIXに接続する場合のデバッグ](#)

```
crypto_isakmp_process_block:src:10.48.68.2,
dest:209.165.200.225 spt:500 dpt:500OAK_AG exchange
ISAKMP (0): processing SA payload. message ID = 0
ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy
ISAKMP:      encryption AES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 2
ISAKMP:      extended auth pre-share (init)
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP:      keylength of 256
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 2 against priority 10 policy
ISAKMP:      encryption AES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 2
ISAKMP:      extended auth pre-share (init)
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP:      keylength of 256
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 3 against priority 10 policy
ISAKMP:      encryption AES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 2
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP:      keylength of 256
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 4 against priority 10 policy
ISAKMP:      encryption AES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 2
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP:      keylength of 256
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 5 against priority 10 policy
ISAKMP:      encryption AES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 2
ISAKMP:      extended auth pre-share (init)
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP:      keylength of 128
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 6 against priority 10 policy
ISAKMP:      encryption AES-CBC
```

```
ISAKMP:      hash MD5
ISAKMP:      default group 2
ISAKMP:      extended auth pre-share (init)
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP:      keylength of 128
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 7 against priority 10 policy
ISAKMP:      encryption AES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 2
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP:      keylength of 128
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 8 against priority 10 policy
ISAKMP:      encryption AES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 2
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP:      keylength of 128
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 9 against priority 10 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 2
ISAKMP:      extended auth pre-share (init)
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable.
crypto_isakmp_process_block:src:10.48.68.2, dest:209.165.200.225 spt:500 dpt:500
crypto_isakmp_process_block:src:10.48.68.2, dest:209.165.200.225 spt:500 dpt:500
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 10.48.68.2.message ID = 17138612
ISAKMP: Config payload CFG_REPLY return status is IKMP_ERR_NO_RETRANS
ISAKMP (0:0): initiating peer config to 10.48.68.2. ID = 134858975 (0x809c8df)
crypto_isakmp_process_block:src:10.48.68.2, dest:209.165.200.225 spt:500 dpt:500
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 10.48.68.2. message ID = 17138612
ISAKMP: Config payload CFG_ACK
return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:10.48.68.2, dest:209.165.200.225 spt:500 dpt:500
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 10.48.68.2. message ID = 17138612
ISAKMP: Config payload CFG_REQUEST
ISAKMP (0:0): checking request:
ISAKMP: attribute      IP4_ADDRESS (1)
ISAKMP: attribute      IP4_NETMASK (2)
ISAKMP: attribute      IP4_DNS (3)
ISAKMP: attribute      IP4_NBNS (4)
ISAKMP: attribute      ADDRESS_EXPIRY (5)
      Unsupported Attr: 5
ISAKMP: attribute      UNKNOWN (28672)
      Unsupported Attr: 28672
ISAKMP: attribute      UNKNOWN (28673)
      Unsupported Attr: 28673
ISAKMP: attribute      ALT_DEF_DOMAIN (28674)
ISAKMP: attribute      ALT_SPLIT_INCLUDE (28676)
ISAKMP: attribute      ALT_SPLITDNS_NAME (28675)
ISAKMP: attribute      ALT_PFS (28679)
ISAKMP: attribute      ALT_BACKUP_SERVERS (28681)
```

```
ISAKMP: attribute      APPLICATION_VERSION (7)
ISAKMP: attribute      UNKNOWN (28680)
        Unsupported Attr: 28680
ISAKMP: attribute      UNKNOWN (28682)
        Unsupported Attr: 28682
ISAKMP: attribute      UNKNOWN (28677)
        Unsupported Attr: 28677
ISAKMP (0:0): responding to peer config from 10.48.68.2. ID = 1128513895
return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:10.48.68.2, dest:209.165.200.225 spt:500 dpt:500
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 3681346539
ISAKMP : Checking IPsec proposal 1
ISAKMP: transform 1, ESP_AES
ISAKMP:  attributes in transform:
ISAKMP:     authenticator is HMAC-MD5
ISAKMP:     key length is 256
ISAKMP:     encaps is 1
ISAKMP:     SA life type in seconds
ISAKMP:     SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
IPSEC(validate_proposal): transform proposal (prot 3, trans 12, hmac_alg 1) not supported
ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP (0): skipping next ANDed proposal (1)
ISAKMP : Checking IPsec proposal 2
ISAKMP: transform 1, ESP_AES
ISAKMP:  attributes in transform:
ISAKMP:     authenticator is HMAC-SHA
ISAKMP:     key length is 256
ISAKMP:     encaps is 1
ISAKMP:     SA life type in seconds
ISAKMP:     SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
IPSEC(validate_proposal): transform proposal (prot 3, trans 12, hmac_alg 2) not supported
ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP (0): skipping next ANDed proposal (2)
crypto_isakmp_process_block:src:10.48.68.2, dest:209.165.200.225 spt:500 dpt:500
hub(config)#
hub(config)#
hub(config)#
hub(config)#
crypto_isakmp_process_block:src:10.48.68.2, dest:209.165.200.225 spt:500 dpt:500
ISAKMP (0): processing NOTIFY payload 36136 protocol 1
        spi 0, message ID = 3784834735
ISAKMP (0): received DPD_R_U_THERE from peer 10.48.68.2
ISAKMP (0): sending NOTIFY message 36137 protocol 1
return status is IKMP_NO_ERR_NO_TRANS
```

[関連情報](#)

- [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](#)
- [Cisco Secure ACS for Windows に関するサポート ページ](#)
- [PIX コマンド リファレンス](#)
- [PIX に関するサポート ページ](#)
- [IOS での TACACS+ に関するドキュメント](#)
- [TACACS+ に関するサポート ページ](#)
- [Requests for Comments \(RFCs\)](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)