

IPSec を使用した Cisco Secure PIX Firewall 6.0 および Cisco VPN クライアントの設定

目次

[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](#)

[PIX の設定](#)

[Cisco VPN Client](#)

[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](#)

[debug 出力例](#)

[関連情報](#)

概要

Cisco Secure PIX Firewall ソフトウェア リリース 6.0 以降では、Cisco VPN Client 3.x および 4.x からの接続をサポートします。この設定例では、トンネルのエンドポイントとして PIX を使用してトラフィックを接続および暗号化する VPN Client の 2 種類のバージョンを示します。この設定では、IP Security (IPSec) 用に割り当てられるようにアドレスのプールを設定しています。

前提条件

要件

この設定例は PIX が適切な統計、コンジット、またはアクセスリストと既に動作していると仮定します。この資料はこれらの基本概念を説明するように、Cisco VPN Client からの PIX への接続を示すように意図されていません。

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くものです。

- PIXソフトウェアリリース 6.2(1)注: このセットアップは PIXソフトウェアリリース 6.2(1) でテストされましたり、以前のリリースで 6.0(1) に戻って、また新しいリリース動作する必要

があります。

- Cisco VPN Clientバージョン 3.6 Rel注: このセットアップは VPN クライアント v4.0 Rel でテストされましたり、以前のリリースで 3.0 に戻っておよび現在のバージョンまで動作する必要があります。

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たものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

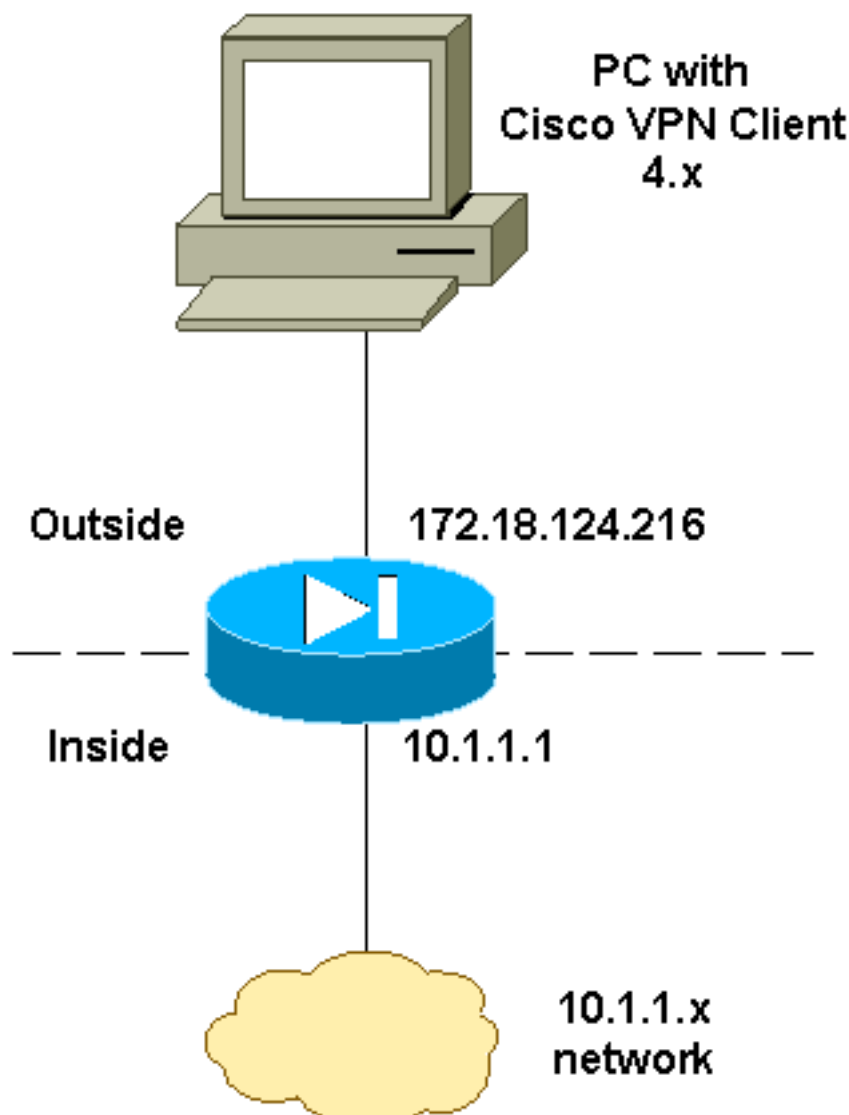
ドキュメント表記の詳細は、『[シスコテクニカルティップスの表記法](#)』を参照してください。

設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



PIX の設定

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。

PIX

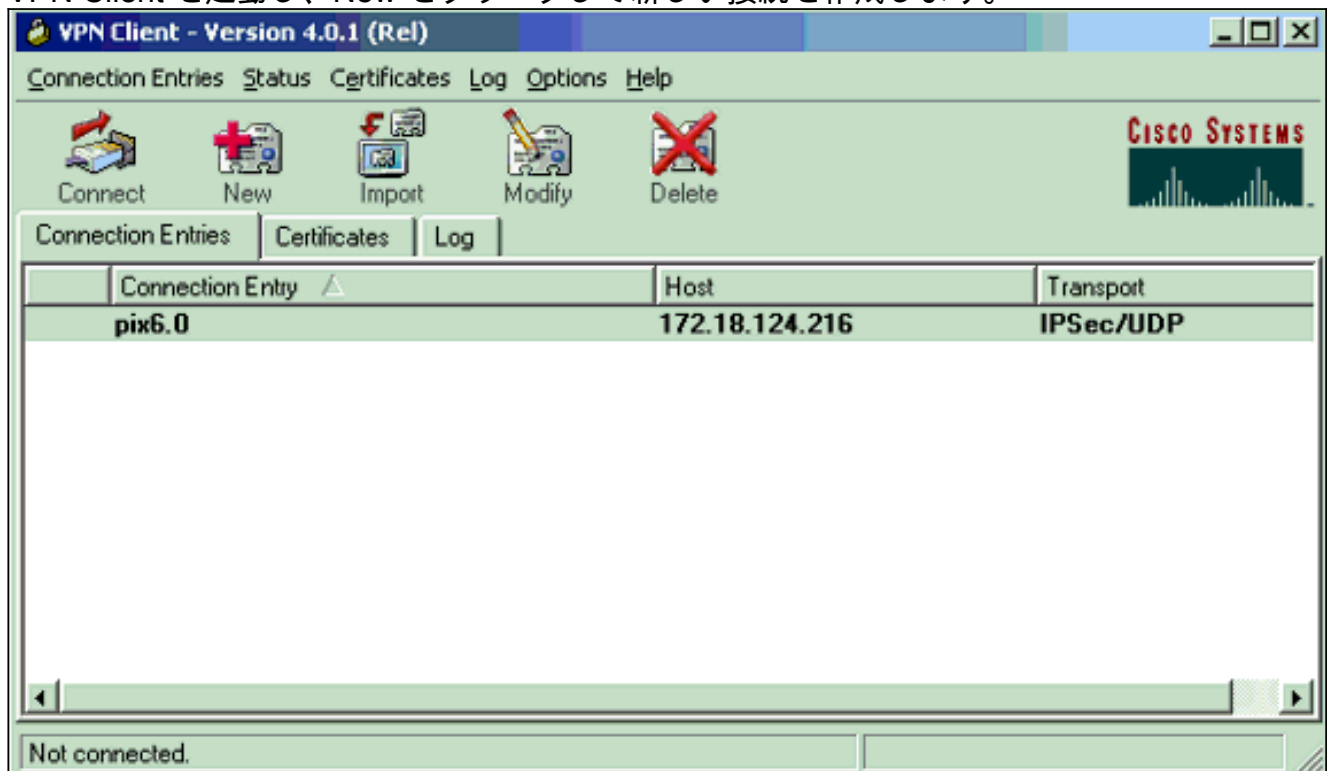
```
PIX Version 6.2(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password OnTrBUG1Tp0edmkr encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname goss-d3-pix515b
domain-name rtp.cisco.com
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
!
!--- Access list to avoid Network Address Translation
(NAT) !--- on the IPsec packets. access-list 101 permit
ip 10.1.1.0 255.255.255.0 10.1.2.0 255.255.255.0 pager
lines 24 interface ethernet0 auto interface ethernet1
auto mtu outside 1500 mtu inside 1500 ! !--- IP
addresses on the interfaces ip address outside
172.18.124.216 255.255.255.0 ip address inside 10.1.1.1
255.255.255.0 ip audit info action alarm ip audit attack
action alarm ip local pool ippool 10.1.2.1-10.1.2.254 no
failover failover timeout 0:00:00 failover poll 15
failover ip address outside 0.0.0.0 failover ip address
inside 0.0.0.0 pdm history enable arp timeout 14400 ! !-
-- Binding ACL 101 to the NAT statement to avoid NAT !--
- on the IPsec packets. nat (inside) 0 access-list 101 !
!--- Default route to the Internet. route outside
0.0.0.0 0.0.0.0 172.18.124.1 1 timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h323 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 http
server enable http 1.2.3.5 255.255.255.255 inside no
snmp-server location no snmp-server contact snmp-server
community public no snmp-server enable traps floodguard
enable ! !--- The sysopt command avoids conduit !--- on
the IPsec encrypted traffic. sysopt connection permit-
ipsec no sysopt route dnat ! !--- Phase 2 encryption
type crypto ipsec transform-set myset esp-des esp-md5-
hmac crypto dynamic-map dynmap 10 set transform-set
myset crypto map mymap 10 ipsec-isakmp dynamic dynmap !
!--- Binding the IPsec engine on the outside interface.
crypto map mymap interface outside ! !--- Enabling
Internet Security Association and !--- Key Management
Protocol (ISAKMP) key exchange. isakmp enable outside
isakmp identity address ! !--- ISAKMP policy for VPN
Client running 3.x or 4.x code. 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 ! !--- IPsec group
configuration for either VPN Client. vpngroup vpn3000
```

```
address-pool ippool vpngroup vpn3000 dns-server 10.1.1.2
vpngroup vpn3000 wins-server 10.1.1.2 vpngroup vpn3000
default-domain cisco.com vpngroup vpn3000 idle-time 1800
vpngroup vpn3000 password ***** !--- To allow
simultaneous access to the !--- internal network and to
the Internet. vpngroup vpn3000 split-tunnel 101 telnet
timeout 5 ssh timeout 5 terminal width 80
Cryptochecksum:94da63fc0bb8ce167407b3ea21c6642c : end
[OK]
```

Cisco VPN Client

VPN クライアントを使用して新しい接続を作成するためにこれらのステップを完了して下さい。

1. VPN Client を起動し、New をクリックして新しい接続を作成します。



2. 新しい接続に関する設定情報を入力します。Connection Entry フィールドでは、エントリに名前を割り当てて下さい。[Host] フィールドでは、PIX のパブリックインターフェイスの IP アドレスを入力して下さい。Authentication タブを選択し、次にグループおよびパスワードを入力して下さい (二度-確認のために...)。終わったら、『SAVE』をクリックして下さい

VPN Client | Create New VPN Connection Entry

Connection Entry:

Description:

Host:

Authentication | Transport | Backup Servers | Dial-Up

Group Authentication

Name:

Password:

Confirm Password:

Certificate Authentication

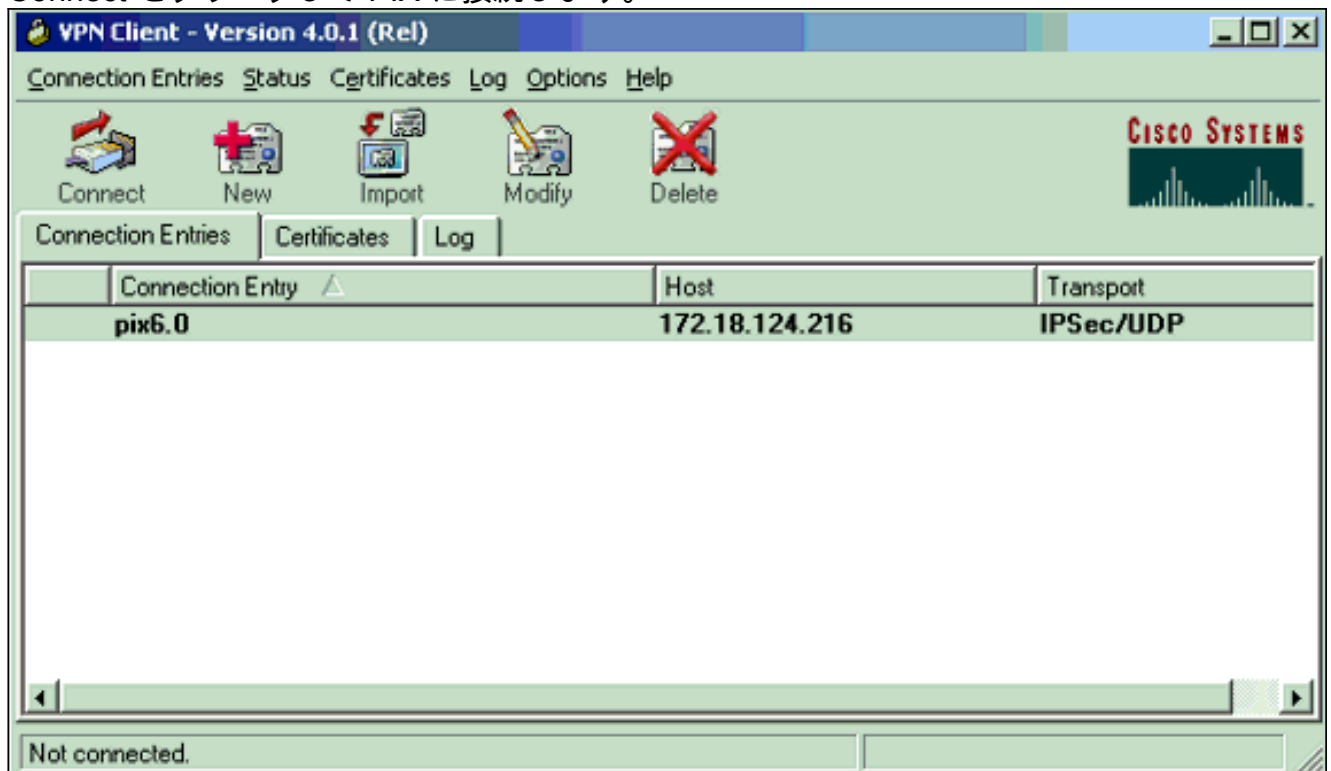
Name:

Send CA Certificate Chain

Erase User Password | Save | Cancel

い。

3. Connect をクリックして PIX に接続します。



確認

ここでは、設定が正常に動作していることを確認します。

[Output Interpreter Tool](#) (OIT) ([登録ユーザ専用](#)) では、特定の **show** コマンドがサポートされています。OIT を使用して、**show** コマンド出力の解析を表示できます。

- **show crypto isakmp sa** — ピアですべての現在のインターネット キー エクスチェンジ (IKE) Security Association (SA) を表示して下さい。
- **show crypto ipsec sa** — 電流 SA によって使用される設定を表示して下さい。

[トラブルシューティング](#)

ここでは、設定に関するトラブルシューティングについて説明します。

[トラブルシューティングのためのコマンド](#)

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 crypto ipsec** : フェーズ 2 の IPsec ネゴシエーションを表示します。
- **debug crypto isakmp** — フェーズ1 の ISAKMP ネゴシエーションを見るのに使用して下さい。
- **debug crypto engine** : 暗号化されたトラフィックを表示します。

[debug 出力例](#)

これは Cisco VPN 3.0.X クライアントと生成される正常な デバッグのサンプルです:

```
goss-d3-pix515b#debug crypto isakmp goss-d3-pix515b#debug crypto ipsec goss-d3-pix515b#debug crypto engine goss-d3-pix515b#show debug debug crypto ipsec 1 debug crypto isakmp 1 debug crypto engine fover status tx Off rx Off open Off cable Off txdmp Off rxdmp Off ifc Off rxip Off txip Off get Off put Off verify Off switch Off fail Off fmsg Off goss-d3-pix515b# goss-d3-pix515b# crypto_isakmp_process_block: src 172.18.124.96, dest 172.18.124.216 OAK_AG exchange ISAKMP (0): processing SA payload. message ID = 0 ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy ISAKMP: encryption 3DES-CBC ISAKMP: hash SHA ISAKMP: default group 2 ISAKMP: extended auth pre-share ISAKMP: life type in seconds ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b ISAKMP (0): atts are not acceptable. Next payload is 3 ISAKMP (0): Checking ISAKMP transform 2 against priority 10 policy ISAKMP: encryption 3DES-CBC ISAKMP: hash MD5 ISAKMP: default group 2 ISAKMP: extended auth pre-share ISAKMP: life type in seconds ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b ISAKMP (0): atts are not acceptable. Next payload is 3 ISAKMP (0): Checking ISAKMP transform 3 against priority 10 policy ISAKMP: encryption 3DES-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 (0): atts are not acceptable. Next payload is 3 ISAKMP (0): Checking ISAKMP transform 4 against priority 10 policy ISAKMP: encryption 3DES-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 (0): atts are not acceptable. Next payload is 3 ISAKMP (0): Checking ISAKMP transform 5 against priority 10 policy ISAKMP: encryption DES-CBC ISAKMP: hash SHA ISAKMP: default group 2 ISAKMP: extended auth pre-share ISAKMP: life type in seconds ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b ISAKMP (0): atts are not acceptable. Next payload is 3 ISAKMP (0): Checking ISAKMP transform 6 against priority 10 policy ISAKMP: encryption DES-CBC ISAKMP: hash MD5 ISAKMP: default group 2 ISAKMP: extended auth pre-share ISAKMP: life type in seconds ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b ISAKMP (0): atts are not acceptable. Next payload is 3 ISAKMP (0): Checking ISAKMP transform 7 against priority 10 policy ISAKMP: encryption DES-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 (0): atts are not acceptable. Next payload is 3 ISAKMP (0): Checking ISAKMP transform 8 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 0x20 0xc4 0x9b ISAKMP (0): atts are acceptable. Next payload is 0 ISAKMP
```

(0): processing KE payload. message ID = 0 ISAKMP (0): processing NONCE payload. message ID = 0
ISAKMP (0): processing ID payload. message ID = 0 ISAKMP (0): processing vendor id payload
ISAKMP (0): processing vendor id payload ISAKMP (0): remote peer supports dead peer detection
ISAKMP (0): processing vendor id payload ISAKMP (0): speaking to a Unity client ISAKMP: Created
a peer node for 172.18.124.96 ISAKMP (0): ID payload next-payload : 10 type : 1 protocol : 17
port : 500 length : 8 ISAKMP (0): Total payload length: 12 return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.18.124.96, dest 172.18.124.216 OAK_AG exchange ISAKMP (0):
processing HASH payload. message ID = 0 ISAKMP (0): processing NOTIFY payload 24578 protocol 1
spi 0, message ID = 0 ISAKMP (0): processing notify INITIAL_CONTACT IPSEC(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 172.18.124.96 ISAKMP (0): SA has been
authenticated return status is IKMP_NO_ERROR crypto_isakmp_process_block: src 172.18.124.96,
dest 172.18.124.216 ISAKMP_TRANSACTION exchange ISAKMP (0:0): processing transaction payload
from 172.18.124.96. message ID = 0 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 APPLICATION_VERSION (7) Unsupported Attr: 7 ISAKMP: attribute UNKNOWN
(28672) Unsupported Attr: 28672 ISAKMP: attribute UNKNOWN (28673) Unsupported Attr: 28673
ISAKMP: attribute UNKNOWN (28674) ISAKMP: attribute UNKNOWN (28676) ISAKMP: attribute UNKNOWN
(28679) Unsupported Attr: 28679 ISAKMP (0:0): responding to peer config from 172.18.124.96. ID =
525416177 return status is IKMP_NO_ERROR crypto_isakmp_process_block: src 172.18.124.96, dest
172.18.124.216 OAK_QM exchange oakley_process_quick_mode: OAK_QM_IDLE ISAKMP (0): processing SA
payload. message ID = 805890102 ISAKMP : Checking IPsec proposal 1 ISAKMP: transform 1, ESP_3DES
ISAKMP: attributes in transform: ISAKMP: authenticator is HMAC-MD5 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 3, 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_3DES ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-SHA 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 3, hmac_alg 2) not supported ISAKMP (0): atts not acceptable. Next payload is 0 ISAKMP
(0): skipping next ANDED proposal (2) ISAKMP : Checking IPsec proposal 3 ISAKMP: transform 1,
ESP_3DES ISAKMP: attributes in transform: ISAKMP: authenticator is HMAC-MD5 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 3, hmac_alg 1) not supported ISAKMP
(0): atts not acceptable. Next payload is 0 ISAKMP : Checking IPsec proposal 4 ISAKMP: transform
1, ESP_3DES ISAKMP: attributes in transform: ISAKMP: authenticator is HMAC-SHA 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 3, hmac_alg 2) not supported ISAKMP
(0): atts not acceptable. Next payload is 0 ISAKMP : Checking IPsec proposal 5 ISAKMP: transform
1, ESP_DES ISAKMP: attributes in transform: ISAKMP: authenticator is HMAC-MD5 ISAKMP: encaps is
1 ISAKMP: SA life type in seconds ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b ISAKMP
(0): atts are acceptable. ISAKMP (0): bad SPI size of 2 octets! ISAKMP : Checking IPsec proposal
6 ISAKMP: transform 1, ESP_DES ISAKMP: attributes in transform: ISAKMP: authenticator is HMAC-
SHA 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 2, hmac_alg 2) not
supported ISAKMP (0): atts not acceptable. Next payload is 0 ISAKMP (0): skipping next ANDED
proposal (6) ISAKMP : Checking IPsec proposal 7 ISAKMP: transform 1, ESP_DES ISAKMP: attributes
in transform: ISAKMP: authenticator is HMAC-MD5 ISAKMP: encaps is 1 ISAKMP: SA life type in
seconds ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b **ISAKMP (0): atts are acceptable.**
IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) dest= 172.18.124.216, src=
172.18.124.96, dest_proxy= 172.18.124.216/255.255.255.255/0/0 (type=1), src_proxy=
10.1.2.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur=
0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 ISAKMP (0): processing NONCE
payload. message ID = 805890102 ISAKMP (0): processing ID payload. message ID = 805890102 ISAKMP
(0): ID_IPV4_ADDR src 10.1.2.1 prot 0 port 0 ISAKMP (0): processing ID payload. message ID =
805890102 ISAKMP (0): ID_IPV4_ADDR dst 172.18.124.216 prot 0 port 0 IPSEC(key_engine): got a
queue event... IPSEC(spi_response): getting spi 0x13b00d31(330304817) for SA from 172.18.124.96
to 172.18.124.216 for prot 3 return status is IKMP_NO_ERROR crypto_isakmp_process_block: src
172.18.124.96, dest 172.18.124.216 OAK_QM exchange oakley_process_quick_mode: OAK_QM_IDLE ISAKMP
(0): processing SA payload. message ID = 935083707 ISAKMP : Checking IPsec proposal 1 ISAKMP:
transform 1, ESP_3DES ISAKMP: attributes in transform: ISAKMP: authenticator is HMAC-MD5
crypto_isakmp_process_block: src 172.18.124.96, dest 172.18.124.216 OAK_QM exchange
oakley_process_quick_mode: OAK_QM_AUTH_AWAITmap_alloc_entry: allocating entry 1 map_alloc_entry:

```
allocating entry 2 ISAKMP (0): Creating IPsec SAs inbound SA from 172.18.124.96 to
172.18.124.216 (proxy 10.1.2.1 to 172.18.124.216) has spi 330304817 and conn_id 1 and flags 4
lifetime of 2147483 seconds outbound SA from 172.18.124.216 to 172.18.124.96 (proxy
172.18.124.216 to 10.1.2.1) has spi 2130279708 and conn_id 2 and flags 4 lifetime of 2147483
secondsIPSEC(key_engine): got a queue event... IPSEC(initialize_sas): , (key eng. msg.) dest=
172.18.124.216, src= 172.18.124.96, dest_proxy= 172.18.124.216/0.0.0.0/0/0 (type=1), src_proxy=
10.1.2.1/0.0.0.0/0/0 (type=1), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur=
2147483s and 0kb, spi= 0x13b00d31(330304817), conn_id= 1, keysize= 0, flags= 0x4
IPSEC(initialize_sas): , (key eng. msg.) src= 172.18.124.216, dest= 172.18.124.96, src_proxy=
172.18.124.216/0.0.0.0/0/0 (type=1), dest_proxy= 10.1.2.1/0.0.0.0/0/0 (type=1), protocol= ESP,
transform= esp-des esp-md5-hmac , lifedur= 2147483s and 0kb, spi= 0x7ef97d1c(2130279708),
conn_id= 2, keysize= 0, flags= 0x4 return status is IKMP_NO_ERROR crypto_isakmp_process_block:
src 172.18.124.96, dest 172.18.124.216 OAK_QM exchange oakley_process_quick_mode:
OAK_QM_AUTH_AWAITmap_alloc_entry: allocating entry 3 map_alloc_entry: allocating entry 4 ISAKMP
(0): Creating IPsec SAs inbound SA from 172.18.124.96 to 172.18.124.216 (proxy 10.1.2.1 to
0.0.0.0) has spi 4139858833 and conn_id 3 and flags 4 lifetime of 2147483 seconds outbound SA
from 172.18.124.216 to 172.18.124.96 ( proxy 0.0.0.0 to 10.1.2.1) has spi 1487433401 and conn_id
4 and flags 4 lifetime of 2147483 seconds IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): , (key eng. msg.) dest= 172.18.124.216, src= 172.18.124.96, dest_proxy=
0.0.0.0/0.0.0.0/0/0 (type=4), src_proxy= 10.1.2.1/0.0.0.0/0/0 (type=1), protocol= ESP,
transform= esp-des esp-md5-hmac , lifedur= 2147483s and 0kb, spi= 0xf6IPSEC(initialize_sas): ,
(key eng. msg.) src= 172.18.124.216, dest= 172.18.124.96, src_proxy= 0.0.0.0/0.0.0.0/0/0
(type=4), dest_proxy= 10.1.2.1/0.0.0.0/0/0 (type=1), protocol= ESP, transform= esp-des esp-md5-
hmac , lifedur= 2147483s and 0kb, spi= 0x58a86eb9(1487433401), conn_id= 4, keysize= 0, flags=
0x4 return status is IKMP_NO_ERROR crypto_isakmp_process_block: src 172.18.124.96, dest
172.18.124.216 ISAKMP (0): processing NOTIFY payload 36136 protocol 1 spi 0, message ID =
1617869510 ISAMKP (0): received DPD_R_U_THERE from peer 172.18.124.96 ISAKMP (0): sending NOTIFY
message 36137 protocol 1 return status is IKMP_NO_ERR_NO_TRANS goss-d3-pix515b# goss-d3-pix515b#
goss-d3-pix515b#no debug crypto isakmp goss-d3-pix515b#no debug crypto ipsec goss-d3-pix515b#no
debug crypto engine goss-d3-pix515b#
```

関連情報

- [IPSec に関するサポートページ \(英語 \)](#)
- [Cisco Secure PIX ファイアウォール コマンド リファレンス](#)
- [Cisco PIX 500 シリーズ セキュリティ アプライアンス サポート ページ](#)
- [Request for Comments \(RFC \)](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)