nat 0 access-list コマンドを使用した、ルータと PIX 間の IPSec 設定

目次

概要

この文書では、ルータと Cisco Secure PIX Firewall 間の Cisco IP Security（IPSec）の設定について説明します。 本社の LAN とリモート LAN 間でのトラフィックの引き渡しにはプライベートの内部 IP アドレスを使用します。また、ユーザがインターネットにアクセスするとき、LAN ホストを、ルーティング可能な IP アドレスに変換するのにも使用します。 しかし、ユーザは route-map コマンドを使用することで、トラフィックをトンネル伝送することなくインターネット上のパブリック ページにアクセスすることもできます。

『ASA/PIX: IOSルータ LAN間IPSECトンネル 設定例へのセキュリティ アプライアンス モデル詳細をシナリオについて学ぶためルータと Ciscoセキュリティ アプライアンス PIX/ASA 間の LAN-to-LAN トンネル。

はじめに

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。

前提条件

このドキュメントに関する固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くものです。

- Cisco IOS(R) ソフトウェア リリース 12.0(7)T を搭載した Cisco ルータ
- Cisco ルータ PIX ファイアウォール バージョン 5.1(1)

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。 対象のネットワークが実稼働中である場合には、どのような作業についても、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。

背景理論

PIX では、**access-list** および **nat 0** コマンドが連携して機能します。 10.1.1.0 ネットワーク上のユーザが 10.2.2.0 ネットワークにアクセスするときには、10.1.1.0 ネットワークのトラフィックを許可するアクセス リストを使用して、このトラフィックを Network Address Translation（NAT; ネットワーク アドレス変換）変換せずに暗号化します。 しかし、同じユーザが他の場所にアクセスするときには、Port Address Translation（PAT; ポート アドレス変換）によってアドレス 172.17.63.210 に変換します。 ルータでは、10.2.2.0 ネットワークのトラフィックを NAT 変換せずに暗号化することを許可するために、**route-map** コマンドと **access-list** コマンドが使用されます。 しかし、同じユーザが他の場所にアクセスするときには、Port Address Translation（PAT; ポート アドレス変換）によってアドレス 172.17.63.210 に変換します。

トンネル上でトラフィックを PAT 変換せず、インターネットへのトラフィックを PAT 変換するためには、PIX ファイアウォールに次の設定コマンドが必要です。

```
access-list nonat permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0 nat (inside) 0 access-list nonat nat (inside) 1 10.1.1.0 255.255.255.0 0 0
```

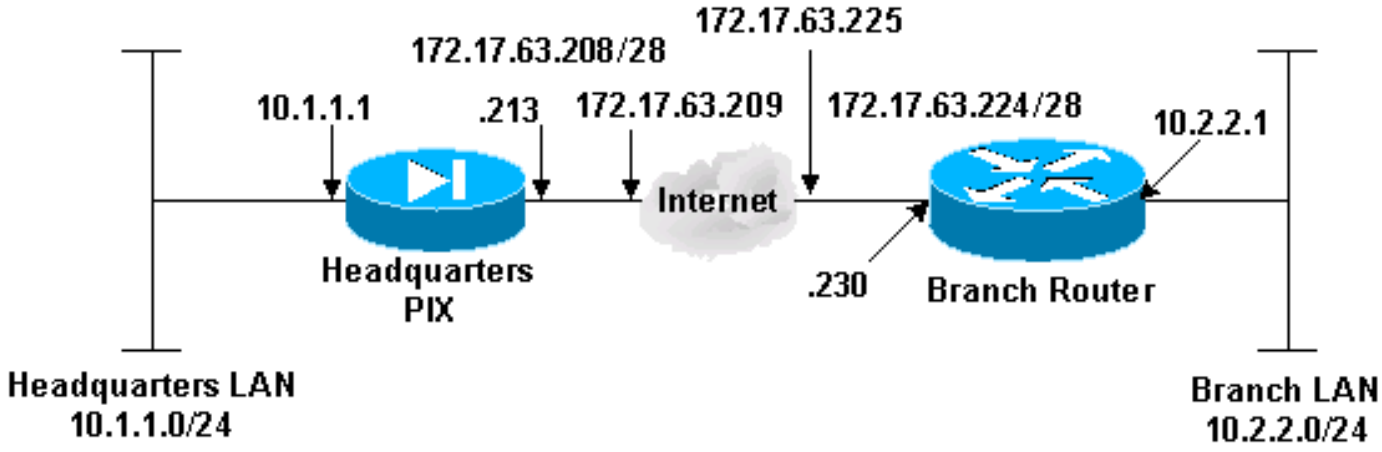
設定

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。

注: このドキュメントで使用されているコマンドに関する詳細情報について調べるには、IOS Command Lookup ツールを使用してください。

ネットワーク図

このドキュメントでは次の図に示すネットワーク



設定

このドキュメントでは次に示す設定を使用しています。

本社の PIX

```
PIX Version 5.1(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
!--- Traffic to the router: access-list ipsec permit ip
10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0 !--- Do
not Network Address Translate (NAT) traffic to the
router: access-list nonat permit ip 10.1.1.0
255.255.255.0 10.2.2.0 255.255.255.0 enable password
8Ry2YjIyt7RRXU24 encrypted passwd 2KFQnbNIdI.2KYOU
encrypted hostname HQ_PIX fixup protocol ftp 21 fixup
protocol http 80 fixup protocol smtp 25 fixup protocol
h323 1720 fixup protocol rsh 514 fixup protocol sqlnet
1521 names pager lines 24 no logging timestamp no
logging standby no logging console no logging monitor no
logging buffered no logging trap no logging history
logging facility 20 logging queue 512 interface
ethernet0 auto interface ethernet1 auto mtu outside 1500
mtu inside 1500 ip address outside 172.17.63.213
255.255.255.240 ip address inside 10.1.1.1 255.255.255.0
no failover failover timeout 0:00:00 failover ip address
outside 0.0.0.0 failover ip address inside 0.0.0.0 arp
timeout 14400 global (outside) 1 172.17.63.210 !--- Do
not NAT traffic to the router: nat (inside) 0 access-
list nonat nat (inside) 1 10.1.1.0 255.255.255.0 0 0
conduit permit icmp any any route outside 0.0.0.0
0.0.0.0 172.17.63.209 1 timeout xlate 3:00:00 conn
1:00:00 half-closed 0:10:00 udp 0:02:00 timeout rpc
0:10:00 h323 0:05:00 timeout uauth 0:05:00 absolute aaa-
server TACACS+ protocol tacacs+ aaa-server RADIUS
protocol radius aaa-server partner protocol tacacs+ no
snmp-server location no snmp-server contact snmp-server
community public no snmp-server enable traps floodguard
enable !--- IPSec policies: sysopt connection permit-
ipsec crypto ipsec transform-set avalanche esp-des esp-
md5-hmac crypto ipsec security-association lifetime
seconds 3600 crypto map forsberg 21 ipsec-isakmp crypto
map forsberg 21 match address ipsec crypto map forsberg
21 set peer 172.17.63.230 crypto map forsberg 21 set
transform-set avalanche crypto map forsberg interface
outside !--- IKE policies: isakmp enable outside isakmp
```

```
key westernfinal2000 address 172.17.63.230 netmask
255.255.255.255 isakmp identity address isakmp policy 21
authentication pre-share isakmp policy 21 encryption des
isakmp policy 21 hash md5 isakmp policy 21 group 1
telnet timeout 5 terminal width 80
Cryptochecksum:e36245da9428c4c07b489f787c8ccd3b : end
```

ブランチ ルータ

```
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Branch_Router
!
!
!
!
!
!
ip subnet-zero
!
!
!--- IKE policies: crypto isakmp policy 11 hash md5
authentication pre-share crypto isakmp key
westernfinal2000 address 172.17.63.213 ! ! !--- IPSec
policies: crypto ipsec transform-set sharks esp-des esp-
md5-hmac ! ! crypto map nolan 11 ipsec-isakmp set peer
172.17.63.213 set transform-set sharks !--- Include the
private-network-to-private-network traffic !--- in the
encryption process. match address 120 ! ! ! interface
Ethernet0 ip address 172.17.63.230 255.255.255.240 no ip
directed-broadcast ip nat outside no ip route-cache
crypto map nolan ! interface Ethernet1 ip address
10.2.2.1 255.255.255.0 no ip directed-broadcast ip nat
inside ! interface Serial0 no ip address no ip directed-
broadcast no ip mroute-cache shutdown no fair-queue !
interface Serial1 no ip address no ip directed-broadcast
shutdown ! ip nat pool branch 172.17.63.230
172.17.63.230 netmask 255.255.255.240 !--- Except the
private network from the NAT process: ip nat inside
source route-map nonat pool branch overload ip classless
ip route 0.0.0.0 0.0.0.0 172.17.63.225 no ip http server
!--- Include the private-network-to-private-network
traffic !--- in the encryption process: access-list 120
permit ip 10.2.2.0 0.0.0.255 10.1.1.0 0.0.0.255 !---
Except the private network from the NAT process: access-
list 130 deny ip 10.2.2.0 0.0.0.255 10.1.1.0 0.0.0.255
access-list 130 permit ip 10.2.2.0 0.0.0.255 any !---
Except the private network from the NAT process: route-
map nonat permit 10 match ip address 130 ! ! line con 0
transport input none line 1 16 line aux 0 line vty 0 4 !
end
```

確認

このセクションでは、設定が正常に動作しているかどうかを確認する際に役立つ情報を提供しています。

特定の **show** コマンドは、アウトプット インタープリタでサポートされています。このツールを使用すると、**show** コマンド出力を分析できます。

- **show crypto isakmp sa**：ピア上の現在の IKE セキュリティ アソシエーション（SA）をすべて表示します。
- show crypto ipsec sa - 現在の（IPSec）SA で使用されている設定を表示します。
- **show crypto engine connections active**：（ルータのみ）現在の接続と、暗号化および復号化されたパケットに関する情報を表示します。

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役立つ情報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

特定の **show** コマンドは、アウトプット インタープリタでサポートされています。このツールを使用すると、**show** コマンド出力を分析できます。

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

両方の IPSec ピアで、次のデバッグを実行している必要があります。

- **debug crypto isakmp**：（ルータおよび PIX）フェーズ 1 中のエラーを表示します。
- **debug crypto ipsec**：（ルータおよび PIX）フェーズ 2 中のエラーを表示します。
- **debug crypto engine**：（ルータのみ）暗号化エンジンからの情報を表示します。

両方のピアで、セキュリティ アソシエーションをクリアする必要があります。 PIX コマンドはイネーブル モードで実行され、 ルータ コマンドは非イネーブル モードで実行されます。

- **clear crypto isakmp sa**：（PIX）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**：（PIX）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。
- **clear crypto isakmp**：（ルータ）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 sa**：（ルータ）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。

デバッグの出力例

- 本社の PIX のデバッグ
- 支店のルータのデバッグ

本社の PIX のデバッグ

```
ISAKMP (0): beginning Main Mode exchange
IPSEC(ipsec_encap): crypto map check deny

02303: sa_request,
  (key eng. msg.) src= 172.17.63.213, dest= 172.17.63.230,
```

```
    src_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
    dest_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 28800s and 4608000kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4004


crypto_isakmp_process_block: src 172.17.63.230,
    dest 172.17.63.213
OAK_MM exchange
ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 1 against priority
    21 policy
ISAKMP:      encryption DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 1
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (basic) of 3600
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_ERRORIPSEC(ipsec_encap): crypto
    map check deny


crypto_isakmp_process_block: src 172.17.63.230,
    dest 172.17.63.213
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): speaking to another IOS box!

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_ERRORIPSEC(ipsec_encap):
    crypto map check deny


crypto_isakmp_process_block: src 172.17.63.230,
    dest 172.17.63.213
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 (0): beginning Quick Mode exchange, M-ID of
   -1448244754:a9ad89eeIPSEC(key_engine): got a
   queue even
IPSEC(spi_response): getting spi 0x5cfcf6e9(1560082153)
    for SA from   172.17.63.230 to
    172.17.63.213 for prot 3

return status is IKMP_NO_ERROR
```

```
crypto_isakmp_process_block: src 172.17.63.230,
    dest 172.17.63.213
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID =
    -1448244754

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= 172.17.63.230,
    src= 172.17.63.213,
    dest_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
    src_proxy= 10.1.1.0/255.255.255.0/0/0 (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 =
     -1448244754

ISAKMP (0): processing ID payload. message ID =
     -1448244754
ISAKMP (0): processing ID payload. message ID =
    -1448244754
ISAKMP (0): processing NOTIFY payload 96 protocol 3
        spi 1510339082, message ID = -1448244754
ISAKMP (0): processing responder lifetime
ISAKMP (0): responder lifetime of
    3600sIPSEC(map_alloc_entry):
    allocating entry 3

IPSEC(map_alloc_entry): allocating entry 4


ISAKMP (0): Creating IPSec SAs
        inbound SA from   172.17.63.230 to
    172.17.63.213
        (proxy 10.2.2.0 to 10.1.1.0)
        has spi 1560082153 and conn_id 3 and flags 4
        lifetime of 3600 seconds
        lifetime of 4608000 kilobytes
        outbound SA from   172.17.63.213 to
    172.17.63.230
        (proxy 10.1.1.0 to 10.2.2.0)
        has spi 183633242 and conn_id 4 and flags 4
        lifetime of 3600 seconds
        lifetime of 4608000 kilobytesIPSEC(key_engine):
    got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 172.17.63.213, src=
    172.17.63.230,
```

```
    dest_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
    src_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x5cfcf6e9(1560082153), conn_id= 3, keysize= 0,
    flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) src= 172.17.63.213, dest=
    172.17.63.230,
    src_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
    dest_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xaf2055a(183633242), conn_id= 4, keysize= 0,
    flags= 0x4

return status is IKMP_NO_ERROR602301: sa created,
  (sa) sa_dest= 172.17.63.213, sa_prot= 50,
    sa_spi= 0x5cfcf6e9(1560082153),
    sa_trans= esp-des esp-md5-hmac , sa_conn_id= 3
602301: sa created,
  (sa) sa_dest= 172.17.63.230, sa_prot= 50,
    sa_spi= 0xaf2055a(183633242),
    sa_trans= esp-des esp-md5-hmac , sa_conn_id= 4
```

支店のルータのデバッグ

```
Branch_Router#
01:27:08: ISAKMP (0): received packet from 172.17.63.213
    (N) NEW SA
01:27:08: ISAKMP (0:1): processing SA payload.
    message ID = 0
01:27:08: ISAKMP (0:1): Checking ISAKMP transform 1
    against priority 11 policy
01:27:08: ISAKMP:      encryption DES-CBC
01:27:08: ISAKMP:      hash MD5
01:27:08: ISAKMP:      default group 1
01:27:08: ISAKMP:      auth pre-share
01:27:08: ISAKMP:      life type in seconds
01:27:08: ISAKMP:      life duration (basic) of 3600
01:27:08: ISAKMP (0:1): atts are acceptable. Next
    payload is 0
01:27:08: CryptoEngine0: generate alg parameter
01:27:10: CRYPTO_ENGINE: Dh phase 1 status: 0
01:27:10: CRYPTO_ENGINE: Dh phase 1 status: 0
01:27:10: ISAKMP (0:1): SA is doing pre-shared key
    authentication
01:27:10: ISAKMP (1): SA is doing pre-shared key
    authentication using id type ID_IPV4_ADDR
01:27:10: ISAKMP (1): sending packet to 172.17.63.213
    (R) MM_SA_SETUP
01:27:10: ISAKMP (1): received packet from 172.17.63.213
    (R) MM_SA_SETUP
01:27:10: ISAKMP (0:1): processing KE payload. message
    ID = 0
01:27:10: CryptoEngine0: generate alg parameter
01:27:12: ISAKMP (0:1): processing NONCE payload.
    message ID = 0
01:27:12: CryptoEngine0: create ISAKMP SKEYID for
    conn id 1
01:27:12: ISAKMP (0:1): SKEYID state generated
01:27:12: ISAKMP (0:1): processing vendor id payload
01:27:12: ISAKMP (0:1): speaking to another IOS box!
01:27:12: ISAKMP (1): sending packet to 172.17.63.213 (R)
```

```
    MM_KEY_EXCH
01:27:12: ISAKMP (1): received packet from 172.17.63.213
    (R) MM_KEY_EXCH
01:27:12: ISAKMP (0:1): processing ID payload.
    message ID = 0
01:27:12: ISAKMP (0:1): processing HASH payload.
    message ID = 0
01:27:12: CryptoEngine0: generate hmac context for
    conn id 1
01:27:12: ISAKMP (0:1): SA has been authenticated
    with 172.17.63.213
01:27:12: ISAKMP (1): ID payload
        next-payload : 8
        type         : 1
        protocol     : 17
        port         : 500
        length       : 8
01:27:12: ISAKMP (1): Total payload length: 12
01:27:12: CryptoEngine0: generate hmac context
    for conn id 1
01:27:12: CryptoEngine0: clear dh number for
    conn id 1
01:27:12: ISAKMP (1): sending packet to
    172.17.63.213 (R) QM_IDLE
01:27:12: ISAKMP (1): received packet from
    172.17.63.213 (R) QM_IDLE
01:27:12: CryptoEngine0: generate hmac context for
    conn id 1
01:27:12: ISAKMP (0:1): processing SA payload.
    message ID = -1448244754
01:27:12: ISAKMP (0:1): Checking IPSec proposal 1
01:27:12: ISAKMP: transform 1, ESP_DES
01:27:12: ISAKMP:   attributes in transform:
01:27:12: ISAKMP:      encaps is 1
01:27:12: ISAKMP:      SA life type in seconds
01:27:12: ISAKMP:      SA life duration (basic)
    of 28800
01:27:12: ISAKMP:      SA life type in kilobytes
01:27:12: ISAKMP:      SA life duration (VPI) of
    0x0 0x46 0x50 0x0
01:27:12: ISAKMP:      authenticator is HMAC-MD5
01:27:12: validate proposal 0
01:27:12: ISAKMP (0:1): atts are acceptable.
01:27:12: IPSEC(validate_proposal_request):
    proposal part #1, (key eng. msg.)
    dest= 172.17.63.230, src= 172.17.63.213,
    dest_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
    src_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
01:27:13: validate proposal request 0
01:27:13: ISAKMP (0:1): processing NONCE payload.
    message ID = -1448244754
01:27:13: ISAKMP (0:1): processing ID payload.
    message ID = -1448244754
01:27:13: ISAKMP (1): ID_IPV4_ADDR_SUBNET src
    10.1.1.0/255.255.255.0 prot 0 port 0
01:27:13: ISAKMP (0:1): processing ID payload.
    message ID = -1448244754
01:27:13: ISAKMP (1): ID_IPV4_ADDR_SUBNET dst
    10.2.2.0/255.255.255.0 prot 0 port 0
01:27:13: IPSEC(key_engine): got a queue event...
01:27:13: IPSEC(spi_response): getting spi 183633242
```

```
    for SA
    from 172.17.63.213 to 172.17.63.230 for prot 3
01:27:13: CryptoEngine0: generate hmac context for
    conn id 1
01:27:13: ISAKMP (1): sending packet to 172.17.63.213
    (R) QM_IDLE
01:27:13: ISAKMP (1): received packet from 172.17.63.213
    (R) QM_IDLE
01:27:13: CryptoEngine0: generate hmac context
    for conn id 1
01:27:13: ipsec allocate flow 0
01:27:13: ipsec allocate flow 0
01:27:13: ISAKMP (0:1): Creating IPSec SAs
01:27:13:         inbound SA from 172.17.63.213
    to 172.17.63.230  (proxy 10.1.1.0 to 10.2.2.0)
01:27:13:         has spi 183633242 and conn_id 2000
    and flags 4
01:27:13:         lifetime of 28800 seconds
01:27:13:         lifetime of 4608000 kilobytes
01:27:13:         outbound SA from 172.17.63.230
    to 172.17.63.213  (proxy 10.2.2.0 to 10.1.1.0)
01:27:13:         has spi 1560082153 and conn_id
    2001 and flags 4
01:27:13:         lifetime of 28800 seconds
01:27:13:         lifetime of 4608000 kilobytes
01:27:13: ISAKMP (0:1): deleting node -1448244754
01:27:13: IPSEC(key_engine): got a queue event...
01:27:13: IPSEC(initialize_sas): ,
   (key eng. msg.) dest= 172.17.63.230, src=
    172.17.63.213,
    dest_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
    src_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 28800s and 4608000kb,
    spi= 0xAF2055A(183633242), conn_id= 2000,
    keysize= 0, flags= 0x4
01:27:13: IPSEC(initialize_sas): ,
   (key eng. msg.) src= 172.17.63.230,
    dest= 172.17.63.213,
    src_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
    dest_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 28800s and 4608000kb,
    spi= 0x5CFCF6E9(1560082153), conn_id= 2001,
    keysize= 0, flags= 0x4
01:27:13: IPSEC(create_sa): sa created,
  (sa) sa_dest= 172.17.63.230, sa_prot= 50,
    sa_spi= 0xAF2055A(183633242),
    sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2000
01:27:13: IPSEC(create_sa): sa created,
  (sa) sa_dest= 172.17.63.213, sa_prot= 50,
    sa_spi= 0x5CFCF6E9(1560082153),
    sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2001
```

関連情報

- PIX IPSec
- Requests for Comments (RFC)
- テクニカルサポート - Cisco Systems