

IOS ルータ : ネットワーク拡張モード (NEM) での Easy VPN (EzVPN) の設定例

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](#)

[設定](#)

[確認](#)

[Cisco 7200 Easy VPN サーバでの show コマンドと出力例](#)

[Cisco 871W Easy VPN リモートでの show コマンドと出力例](#)

[トラブルシューティング](#)

[Easy VPN サーバのコマンド](#)

[Easy VPN リモートのコマンド](#)

[関連情報](#)

概要

このドキュメントでは、Easy VPN (EzVPN) を使用した Cisco 871 ルータと Cisco 7200VXR ルータ間での IPsec の設定例を紹介しています。7200 は Easy VPN サーバ、871 は Easy VPN リモートとして動作します。この例では、プライベート ネットワークとして両方のルータでループバック インターフェイスが使用されています。これらは必要に応じて、ファーストイーサネット やシリアル インターフェイスなどの他のインターフェイスに置き換えが可能です。

Easy VPN を使用して PIX/ASA 7.x と Cisco 871 間に IPsec を設定するには、『[ASA 5500 をサーバ、Cisco 871 を Easy VPN Remote として使用する PIX/ASA 7.x Easy VPN の設定例](#)』を参照してください。

Cisco IOS(R) Easy VPN リモート ハードウェア クライアントと PIX Easy VPN サーバ間に IPsec を設定するには、『[IOS Easy VPN リモート ハードウェア クライアントと PIX Easy VPN サーバの設定例](#)』を参照してください。

Cisco VPN 3000 コンセントレータに接続する Cisco IOS ルータを [Network Extension Mode \(NEM \)](#) で EzVPN として設定するには、『[VPN 3000 コンセントレータに接続する Cisco IOS での Cisco EzVPN クライアントの設定](#)』を参照してください。

前提条件

要件

この設定を試行する前に、IPsec と Cisco 7200/871 のオペレーティング システムに関する基本的な知識があることを確認してください。

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 Easy VPN サーバは、Cisco IOS(R) ソフトウェア リリース 12.4(4)T1 が稼働する 7200 ルータ (VXR) です。
- Cisco Easy VPN リモートは、Cisco IOS ソフトウェア リリース 12.4(2)T1 が稼働する 871W ルータです。

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。

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。

注: ループバック インターフェイスでは内部の PC をシミュレートしています。

設定

このドキュメントでは、次の設定を使用します。

- [Easy VPN サーバ \(Cisco 7200VXR ルータ \)](#)
- [Easy VPN リモート \(Cisco 871W ルータ \)](#)

Easy VPN サーバ (Cisco 7200VXR ルータ)

```
3-07-07-7200VXR#show running-config Building
configuration... Current configuration : 2059 bytes !
version 12.4 service timestamps debug datetime msec
service timestamps log datetime msec no service
password-encryption ! hostname 3-07-07-7200VXR ! boot-
start-marker boot-end-marker ! !--- Enable
Authentication, Authorizing and Accounting (AAA) !---
```

```

for user authentication and group authorization. aaa
new-model ! !--- Enable the AAA commands in order !---
to enable Xauth for user authentication. aaa
authentication login userauthen local !--- Enable the
AAA commands !--- in order to enable group
authorization. aaa authorization network groupauthor
local ! aaa session-id common ! resource policy ! ip
subnet-zero ip cef ! ! !--- Define the username and
password to use for Xauth. username cisco password 0
cisco123 ! ! !--- Create an Internet Security
Association and !--- Key Management Protocol (ISAKMP)
policy for Phase 1 negotiations. crypto isakmp policy 3
encr 3des authentication pre-share group 2 ! ! !---
Create a group with the pre-shared key for IKE
authentication. crypto isakmp client configuration group
vpngrp key cisco123 ! ! !--- Create the Phase 2 policy
for actual data encryption. crypto ipsec transform-set
myset esp-3des esp-sha-hmac ! !--- Create a dynamic map
and !--- apply the transform set that was created
earlier. crypto dynamic-map dynmap 10 set transform-set
myset ! ! !--- Create the actual crypto map, !--- and
apply the AAA lists that were created earlier. !---
These commands associate the AAA commands to the crypto
map. crypto map clientmap client authentication list
userauthen crypto map clientmap isakmp authorization
list groupauthor crypto map clientmap 10 ipsec-isakmp
dynamic dynmap ! ! ! interface Loopback10 ip address
10.10.10.1 255.255.255.0 ! interface GigabitEthernet0/1
ip address 158.100.101.254 255.255.255.0 ip nat inside
ip virtual-reassembly duplex auto speed auto media-type
rj45 no negotiation auto ! interface GigabitEthernet0/2
ip address 158.100.102.254 255.255.255.0 ip nat outside
ip virtual-reassembly duplex auto speed 100 media-type
rj45 no negotiation auto ! ! ! !--- Apply the crypto map
on the interface where !--- traffic leaves the router.
interface GigabitEthernet0/3 ip address 172.16.186.186
255.255.255.0 duplex auto speed auto media-type rj45 no
negotiation auto crypto map clientmap ! interface
FastEthernet1/0 no ip address shutdown duplex half ! ip
default-gateway 172.16.186.1 ip classless ip route
0.0.0.0 0.0.0.0 172.16.186.1 no ip http server no ip
http secure-server ! ! ip nat Stateful id 10 ip nat pool
honnat 158.100.96.90 158.100.96.99 netmask 255.255.255.0
ip nat inside source route-map test pool honnat mapping-
id 10 overload ! logging alarm informational access-list
100 permit ip any any ! route-map test permit 10 match
ip address 100 ! ! ! ! control-plane ! ! ! ! ! !
gatekeeper shutdown ! ! line con 0 logging synchronous
stopbits 1 line aux 0 stopbits 1 line vty 0 4 ! ! end

```

Easy VPN リモート (Cisco 871W ルータ)

```

3-03-06-871W#show running-config Current configuration :
1563 bytes ! version 12.4 no service pad service
timestamps debug datetime msec service timestamps log
datetime msec service password-encryption ! hostname 3-
03-06-871W ! boot-start-marker boot-end-marker ! ! no
aaa new-model ! resource policy ! ip cef ! ! ! ! ip
name-server 171.70.168.183 ! ! username cisco privilege
15 password 7 00071A150754 ! ! ! ! !--- Set the
parameters to connect to the !--- appropriate Easy VPN
group on the Easy VPN server. crypto ipsec client ezvpn
ez connect auto group vpngrp key cisco123 mode network-
extension peer 172.16.186.186 xauth userid mode
interactive ! ! ! !--- Define the inside interfaces that

```

```

will access !--- and can be accessed via Easy VPN.
interface Loopback0 ip address 10.12.130.1
255.255.255.255 crypto ipsec client ezvpn ez inside !
interface FastEthernet0 ! interface FastEthernet1 !
interface FastEthernet2 ! interface FastEthernet3 !---
Use the crypto ipsec client ezvpn <name> command on the
!--- interface that connects to the Easy VPN server !---
in order to complete the Easy VPN. interface
FastEthernet4 ip address 172.16.186.130 255.255.255.0
duplex auto speed auto crypto ipsec client ezvpn ez !
interface Dot11Radio0 no ip address shutdown speed
basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0
18.0 24.0 36.0 48.0 54.0 station-role root ! interface
Vlan1 no ip address ! ip default-gateway 172.16.186.1 ip
route 0.0.0.0 0.0.0.0 172.16.186.1 ! ! no ip http server
no ip http secure-server ! access-list 121 dynamic
testlist permit tcp any host 12.12.12.12 eq 5900 snmp-
server community presto RW ! ! route-map polo permit
10 ! route-map asa permit 10 ! tacacs-server host
66.94.234.13 tacacs-server directed-request ! control-
plane ! ! line con 0 no modem enable line aux 0 line vty
0 4 login ! scheduler max-task-time 5000 ! webvpn
context Default_context ssl authenticate verify all ! no
inservice ! end

```

確認

以降のセクションを使用して、設定が正しく動作していることを確認します。

- [Cisco 7200 Easy VPN サーバでの show コマンドと出力例](#)
- [Cisco 871W Easy VPN リモートでの show コマンドと出力例](#)

[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。

[Cisco 7200 Easy VPN サーバでの show コマンドと出力例](#)

- **show crypto isakmp sa** : ピアにおける現在のインターネット鍵交換 (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。3-07-07-7200VXR#**show crypto isakmp sa** IPv4
Crypto ISAKMP SA dst src state conn-id slot status 172.16.186.186 172.16.186.130 QM_IDLE
1008 0 ACTIVE IPv6 Crypto ISAKMP SA
- **show crypto ipsec sa** : ピア間に構築された IPSec SA を表示します。3-07-07-7200VXR#**show crypto ipsec sa** interface: GigabitEthernet0/3 Crypto map tag: clientmap, local addr
172.16.186.186 protected vrf: (none) local ident (addr/mask/prot/port):
(0.0.0.0/0.0.0.0/0/0) remote ident (addr/mask/prot/port): (10.12.130.1/255.255.255.255/0/0)
current_peer 172.16.186.130 port 500 PERMIT, flags={ } #pkts encaps: 5, #pkts encrypt: 5,
#pkts digest: 5 #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5 #pkts compressed: 0,
#pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0 #pkts not
decompressed: 0, #pkts decompress failed: 0 #send errors 0, #recv errors 0 local crypto
endpt.: 172.16.186.186, remote crypto endpt.: 172.16.186.130 path mtu 1500, ip mtu 1500
current outbound spi: 0x29354010(691355664) inbound esp sas: spi: 0x6875F644(1752561220)
transform: esp-3des esp-sha-hmac , in use settings = {Tunnel, } conn id: 11, flow_id: SW:11,
crypto map: clientmap sa timing: remaining key lifetime (k/sec): (4439946/3526) IV size: 8
bytes replay detection support: Y Status: ACTIVE inbound ah sas: inbound pcp sas: outbound
esp sas: spi: 0x29354010(691355664) transform: esp-3des esp-sha-hmac , in use settings
={Tunnel, } conn id: 12, flow_id: SW:12, crypto map: clientmap sa timing: remaining key
lifetime (k/sec): (4439946/3524) IV size: 8 bytes replay detection support: Y Status: ACTIVE

[Cisco 871W Easy VPN リモートでの show コマンドと出力例](#)

- **show crypto isakmp sa** : 現在ピアにあるすべての IKE SA を表示します。3-03-06-871W#`show crypto isakmp sa` IPv4 Crypto ISAKMP SA dst src state conn-id slot status 172.16.186.186 172.16.186.130 QM_IDLE 2003 0 ACTIVE IPv6 Crypto ISAKMP SA
- **show crypto ipsec sa** : ピア間に構築された IPSec SA を表示します。3-03-06-871W#`show crypto ipsec sa` interface: FastEthernet4 Crypto map tag: FastEthernet4-head-0, local addr 172.16.186.130 protected vrf: (none) local ident (addr/mask/prot/port): (10.12.130.1/255.255.255.255/0/0) remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) current_peer 172.16.186.186 port 500 PERMIT, flags={origin_is_acl,} #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5 #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0 #pkts not decompressed: 0, #pkts decompress failed: 0 #send errors 0, #recv errors 0 local crypto endpt.: 172.16.186.130, remote crypto endpt.: 172.16.186.186 path mtu 1500, ip mtu 1500 current outbound spi: 0x6875F644(1752561220) inbound esp sas: spi: 0x29354010(691355664) transform: esp-3des esp-sha-hmac , in use settings = {Tunnel, } conn id: 11, flow_id: Motorola SEC 1.0:11, crypto map: FastEthernet4-head-0 sa timing: remaining key lifetime (k/sec): (4607687/3531) IV size: 8 bytes replay detection support: Y Status: ACTIVE inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0x6875F644(1752561220) transform: esp-3des esp-sha-hmac , in use settings = {Tunnel, } conn id: 12, flow_id: Motorola SEC 1.0:12, crypto map: FastEthernet4-head-0 sa timing: remaining key lifetime (k/sec): (4607687/3528) IV size: 8 bytes replay detection support: Y Status: ACTIVE outbound ah sas: outbound pcp sas:
- **show crypto ipsec client ezvpn** : Cisco Easy VPN リモートの設定を表示します。3-03-06-871W#`show crypto ipsec client ezvpn` Easy VPN Remote Phase: 6 Tunnel name : ez Inside interface list: Loopback0 Outside interface: FastEthernet4 Current State: IPSEC_ACTIVE Last Event: SOCKET_UP Save Password: Disallowed Current EzVPN Peer: 172.16.186.186 3-03-06-871W#`ping 10.10.10.1 source 10.12.130.1` Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds: Packet sent with a source address of 10.12.130.1 !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

[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。

[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。

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。

Easy VPN リモートと Easy VPN サーバをこのドキュメントの説明どおりに設定しても問題が起る場合は、Cisco Technical Support による分析用に、各デバイスの debug 出力と show コマンドの出力を収集してください。

次のセクションでは debug コマンドと出力例を示します。

- [Easy VPN サーバのコマンド](#)
- [Easy VPN リモートのコマンド](#)

[Easy VPN サーバのコマンド](#)

- `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表示します。

```
3-07-07-7200VXR#debug crypto ipsec 3-07-07-7200VXR#debug crypto isakmp *May 4 00:44:19.389:
IPSEC(key_engine): got a queue event with 1 KMI message(s) *May 4 00:44:20.937: ISAKMP (0:0):
```

received packet from 172.16.186.130 dport 500 sport 500 Global (N) **NEW SA** *May 4 00:44:20.937:
ISAKMP: Created a peer struct for 172.16.186.130, peer port 500 *May 4 00:44:20.937: ISAKMP: New
peer created peer = 0x6745B8E0 peer_handle = 0x80000009 *May 4 00:44:20.937: ISAKMP: Locking
peer struct 0x6745B8E0, refcount 1 for crypto_isakmp_process_block *May 4 00:44:20.937:
ISAKMP:(0):Setting client config settings 6741FF98 *May 4 00:44:20.937: ISAKMP:(0):(Re)Setting
client xauth list and state *May 4 00:44:20.937: ISAKMP/xauth: initializing AAA request *May 4
00:44:20.937: ISAKMP: local port 500, remote port 500 *May 4 00:44:20.937: ISAKMP: Find a dup sa
in the avl tree during calling isadb_insert sa = 67369734 *May 4 00:44:20.937: ISAKMP:(0):
processing SA payload. message ID = 0 *May 4 00:44:20.937: ISAKMP:(0): processing ID payload.
message ID = 0 *May 4 00:44:20.937: ISAKMP (0:0): ID payload next-payload : 13 type : 11 group
id : **vpngrp** protocol : 17 port : 0 length : 14 *May 4 00:44:20.937: ISAKMP:(0):: peer matches
none of the profiles *May 4 00:44:20.937: ISAKMP:(0): processing vendor id payload *May 4
00:44:20.937: ISAKMP:(0): vendor ID seems Unity/DPD but major 245 mismatch *May 4 00:44:20.937:
ISAKMP (0:0): vendor ID is NAT-T v7 *May 4 00:44:20.937: ISAKMP:(0): processing vendor id
payload *May 4 00:44:20.937: ISAKMP:(0): vendor ID seems Unity/DPD but major 157 mismatch *May 4
00:44:20.937: ISAKMP:(0): vendor ID is NAT-T v3 *May 4 00:44:20.937: ISAKMP:(0): processing
vendor id payload *May 4 00:44:20.937: ISAKMP:(0): vendor ID seems Unity/DPD but major 123
mismatch *May 4 00:44:20.937: ISAKMP:(0): vendor ID is NAT-T v2 *May 4 00:44:20.937: ISAKMP:(0):
Authentication by xauth preshared *May 4 00:44:20.937: ISAKMP:(0):Checking ISAKMP transform 1
against priority 3 policy *May 4 00:44:20.937: ISAKMP: encryption AES-CBC *May 4 00:44:20.937:
ISAKMP: keylength of 128 *May 4 00:44:20.937: ISAKMP: hash SHA *May 4 00:44:20.937: ISAKMP:
default group 2 *May 4 00:44:20.937: ISAKMP: auth XAUTHInitPreShared *May 4 00:44:20.937:
ISAKMP: life type in seconds *May 4 00:44:20.937: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4
0x9B *May 4 00:44:20.937: ISAKMP:(0):Encryption algorithm offered does not match policy! *May 4
00:44:20.937: ISAKMP:(0):atts are not acceptable. Next payload is 3 *May 4 00:44:20.937:
ISAKMP:(0):Checking ISAKMP transform 2 against priority 3 policy *May 4 00:44:20.937: ISAKMP:
encryption AES-CBC *May 4 00:44:20.937: ISAKMP: keylength of 128 *May 4 00:44:20.937: ISAKMP:
hash MD5 *May 4 00:44:20.937: ISAKMP: default group 2 *May 4 00:44:20.937: ISAKMP: auth
XAUTHInitPreShared *May 4 00:44:20.937: ISAKMP: life type in seconds *May 4 00:44:20.937:
ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B *May 4 00:44:20.937: ISAKMP:(0):Encryption
algorithm offered does not match policy! *May 4 00:44:20.937: ISAKMP:(0):atts are not
acceptable. Next payload is 3 *May 4 00:44:20.937: ISAKMP:(0):Checking ISAKMP transform 3
against priority 3 policy *May 4 00:44:20.937: ISAKMP: encryption AES-CBC *May 4 00:44:20.937:
ISAKMP: keylength of 192 *May 4 00:44:20.937: ISAKMP: hash SHA *May 4 00:44:20.937: ISAKMP:
default group 2 *May 4 00:44:20.937: ISAKMP: auth XAUTHInitPreShared *May 4 00:44:20.937:
ISAKMP: life type in seconds *May 4 00:44:20.937: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4
0x9B *May 4 00:44:20.937: ISAKMP:(0):Encryption algorithm offered does not match policy! *May 4
00:44:20.937: ISAKMP:(0):atts are not acceptable. Next payload is 3 *May 4 00:44:20.937:
ISAKMP:(0):Checking ISAKMP transform 4 against priority 3 policy *May 4 00:44:20.937: ISAKMP:
encryption AES-CBC *May 4 00:44:20.937: ISAKMP: keylength of 192 *May 4 00:44:20.937: ISAKMP:
hash MD5 *May 4 00:44:20.937: ISAKMP: default group 2 *May 4 00:44:20.937: ISAKMP: auth
XAUTHInitPreShared *May 4 00:44:20.937: ISAKMP: life type in seconds *May 4 00:44:20.937:
ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B *May 4 00:44:20.937: ISAKMP:(0):Encryption
algorithm offered does not match policy! *May 4 00:44:20.937: ISAKMP:(0):atts are not
acceptable. Next payload is 3 *May 4 00:44:20.937: ISAKMP:(0):Checking ISAKMP transform 5
against priority 3 policy *May 4 00:44:20.937: ISAKMP: encryption AES-CBC *May 4 00:44:20.937:
ISAKMP: keylength of 256 *May 4 00:44:20.937: ISAKMP: hash SHA *May 4 00:44:20.937: ISAKMP:
default group 2 *May 4 00:44:20.937: ISAKMP: auth XAUTHInitPreShared *May 4 00:44:20.937:
ISAKMP: life type in seconds *May 4 00:44:20.937: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4
0x9B *May 4 00:44:20.937: ISAKMP:(0):Encryption algorithm offered does not match policy! *May 4
00:44:20.937: ISAKMP:(0):atts are not acceptable. Next payload is 3 *May 4 00:44:20.937:
ISAKMP:(0):Checking ISAKMP transform 6 against priority 3 policy *May 4 00:44:20.937: ISAKMP:
encryption AES-CBC *May 4 00:44:20.937: ISAKMP: keylength of 256 *May 4 00:44:20.941: ISAKMP:
hash MD5 *May 4 00:44:20.941: ISAKMP: default group 2 *May 4 00:44:20.941: ISAKMP: auth
XAUTHInitPreShared *May 4 00:44:20.941: ISAKMP: life type in seconds *May 4 00:44:20.941:
ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B *May 4 00:44:20.941: ISAKMP:(0):Encryption
algorithm offered does not match policy! *May 4 00:44:20.941: ISAKMP:(0):atts are not
acceptable. Next payload is 3 *May 4 00:44:20.941: ISAKMP:(0):Checking ISAKMP transform 7
against priority 3 policy *May 4 00:44:20.941: ISAKMP: encryption AES-CBC *May 4 00:44:20.941:
ISAKMP: keylength of 128 *May 4 00:44:20.941: ISAKMP: hash SHA *May 4 00:44:20.941: ISAKMP:
default group 2 *May 4 00:44:20.941: ISAKMP: auth pre-share *May 4 00:44:20.941: ISAKMP: life
type in seconds *May 4 00:44:20.941: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B *May 4
00:44:20.941: ISAKMP:(0):Encryption algorithm offered does not match policy! *May 4
00:44:20.941: ISAKMP:(0):atts are not acceptable. Next payload is 3 *May 4 00:44:20.941:

ISAKMP:(0):Checking ISAKMP transform 8 against priority 3 policy *May 4 00:44:20.941: ISAKMP: encryption AES-CBC *May 4 00:44:20.941: ISAKMP: keylength of 128 *May 4 00:44:20.941: ISAKMP: hash MD5 *May 4 00:44:20.941: ISAKMP: default group 2 *May 4 00:44:20.941: ISAKMP: auth pre-share *May 4 00:44:20.941: ISAKMP: life type in seconds *May 4 00:44:20.941: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B *May 4 00:44:20.941: ISAKMP:(0):Encryption algorithm offered does not match policy! *May 4 00:44:20.941: ISAKMP:(0):atts are not acceptable. Next payload is 3 *May 4 00:44:20.941: ISAKMP:(0):Checking ISAKMP transform 9 against priority 3 policy *May 4 00:44:20.941: ISAKMP: encryption AES-CBC *May 4 00:44:20.941: ISAKMP: keylength of 192 *May 4 00:44:20.941: ISAKMP: hash SHA *May 4 00:44:20.941: ISAKMP: default group 2 *May 4 00:44:20.941: ISAKMP: auth pre-share *May 4 00:44:20.941: ISAKMP: life type in seconds *May 4 00:44:20.941: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B *May 4 00:44:20.941: ISAKMP:(0):Encryption algorithm offered does not match policy! *May 4 00:44:20.941: ISAKMP:(0):atts are not acceptable. Next payload is 3 *May 4 00:44:20.941: ISAKMP:(0):Checking ISAKMP transform 10 against priority 3 policy *May 4 00:44:20.941: ISAKMP: encryption AES-CBC *May 4 00:44:20.941: ISAKMP: keylength of 192 *May 4 00:44:20.941: ISAKMP: hash MD5 *May 4 00:44:20.941: ISAKMP: default group 2 *May 4 00:44:20.941: ISAKMP: auth pre-share *May 4 00:44:20.941: ISAKMP: life type in seconds *May 4 00:44:20.941: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B *May 4 00:44:20.941: ISAKMP:(0):Encryption algorithm offered does not match policy! *May 4 00:44:20.941: ISAKMP:(0):atts are not acceptable. Next payload is 3 *May 4 00:44:20.941: ISAKMP:(0):Checking ISAKMP transform 11 against priority 3 policy *May 4 00:44:20.941: ISAKMP: encryption AES-CBC *May 4 00:44:20.941: ISAKMP: keylength of 256 *May 4 00:44:20.941: ISAKMP: hash SHA *May 4 00:44:20.941: ISAKMP: default group 2 *May 4 00:44:20.941: ISAKMP: auth pre-share *May 4 00:44:20.941: ISAKMP: life type in seconds *May 4 00:44:20.941: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B *May 4 00:44:20.941: ISAKMP:(0):Encryption algorithm offered does not match policy! *May 4 00:44:20.941: ISAKMP:(0):atts are not acceptable. Next payload is 3 *May 4 00:44:20.941: ISAKMP:(0):Checking ISAKMP transform 12 against priority 3 policy *May 4 00:44:20.941: ISAKMP: encryption AES-CBC *May 4 00:44:20.941: ISAKMP: keylength of 256 *May 4 00:44:20.941: ISAKMP: hash MD5 *May 4 00:44:20.941: ISAKMP: default group 2 *May 4 00:44:20.941: ISAKMP: auth pre-share *May 4 00:44:20.941: ISAKMP: life type in seconds *May 4 00:44:20.941: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B *May 4 00:44:20.941: ISAKMP:(0):Encryption algorithm offered does not match policy! *May 4 00:44:20.941: ISAKMP:(0):atts are not acceptable. Next payload is 3 *May 4 00:44:20.941: ISAKMP:(0):Checking ISAKMP transform 13 against priority 3 policy *May 4 00:44:20.941: ISAKMP: encryption 3DES-CBC *May 4 00:44:20.941: ISAKMP: hash SHA *May 4 00:44:20.941: ISAKMP: default group 2 *May 4 00:44:20.941: ISAKMP: auth XAUTHInitPreShared *May 4 00:44:20.941: ISAKMP: life type in seconds *May 4 00:44:20.941: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B *May 4 00:44:20.941: **ISAKMP:(0):atts are acceptable. Next payload is 3** *May 4 00:44:20.941: ISAKMP:(0): processing vendor id payload *May 4 00:44:20.941: ISAKMP:(0): vendor ID seems Unity/DPD but major 245 mismatch *May 4 00:44:20.941: ISAKMP (0:0): vendor ID is NAT-T v7 *May 4 00:44:20.941: ISAKMP:(0): processing vendor id payload *May 4 00:44:20.941: ISAKMP:(0): vendor ID seems Unity/DPD but major 157 mismatch *May 4 00:44:20.941: ISAKMP:(0): vendor ID is NAT-T v3 *May 4 00:44:20.941: ISAKMP:(0): processing vendor id payload *May 4 00:44:20.941: ISAKMP:(0): vendor ID seems Unity/DPD but major 123 mismatch *May 4 00:44:20.941: ISAKMP:(0): vendor ID is NAT-T v2 *May 4 00:44:20.941: ISAKMP:(0): processing KE payload. message ID = 0 *May 4 00:44:20.957: ISAKMP:(0): processing NONCE payload. message ID = 0 *May 4 00:44:20.957: ISAKMP:(0): processing vendor id payload *May 4 00:44:20.957: ISAKMP:(0): vendor ID is DPD *May 4 00:44:20.957: ISAKMP:(0): processing vendor id payload *May 4 00:44:20.957: ISAKMP:(0): vendor ID seems Unity/DPD but major 79 mismatch *May 4 00:44:20.957: ISAKMP:(0): vendor ID is XAUTH *May 4 00:44:20.957: ISAKMP:(0): processing vendor id payload *May 4 00:44:20.957: ISAKMP:(0): claimed IOS but failed authentication *May 4 00:44:20.957: ISAKMP:(0): processing vendor id payload *May 4 00:44:20.957: ISAKMP:(0): vendor ID is Unity *May 4 00:44:20.957: ISAKMP:(0):Input = IKE_MSG_FROM_PEER, IKE_AM_EXCH *May 4 00:44:20.957: ISAKMP:(0):Old State = IKE_READY New State = IKE_R_AM_AAA_AWAIT *May 4 00:44:20.957: ISAKMP:(1008): constructed NAT-T vendor-07 ID *May 4 00:44:20.957: ISAKMP:(1008):SA is doing pre-shared key authentication plus XAUTH using id type ID_IPV4_ADDR *May 4 00:44:20.957: ISAKMP (0:1008): ID payload next-payload : 10 type : 1 address : 172.16.186.186 protocol : 17 port : 0 length : 12 *May 4 00:44:20.957: ISAKMP:(1008):Total payload length: 12 *May 4 00:44:20.957: ISAKMP:(1008): sending packet to 172.16.186.130 my_port 500 peer_port 500 (R) AG_INIT_EXCH *May 4 00:44:20.957: ISAKMP:(1008):Input = IKE_MSG_FROM_AAA, PRESHARED_KEY_REPLY *May 4 00:44:20.957: ISAKMP:(1008):Old State = IKE_R_AM_AAA_AWAIT New State = IKE_R_AM2 *May 4 00:44:20.985: ISAKMP (0:1008): received packet from 172.16.186.130 dport 500 sport 500 Global (R) AG_INIT_EXCH *May 4 00:44:20.985: ISAKMP:(1008): processing HASH payload. message ID = 0 *May 4 00:44:20.985: ISAKMP:(1008): processing NOTIFY INITIAL_CONTACT protocol 1 spi 0, message ID = 0, sa = 67369734 *May 4 00:44:20.985: ISAKMP:(1008):SA authentication status: authenticated *May 4 00:44:20.985: ISAKMP:(1008):SA has been authenticated with

172.16.186.130 *May 4 00:44:20.985: ISAKMP:(1008):SA authentication status: authenticated *May 4 00:44:20.985: ISAKMP:(1008): Process initial contact, bring down existing phase 1 and 2 SA's with local 172.16.186.186 remote 172.16.186.130 remote port 500 *May 4 00:44:20.985: ISAKMP:(1008):returning IP addr to the address pool *May 4 00:44:20.985: ISAKMP: Trying to insert a peer 172.16.186.186/172.16.186.130/500/, and inserted successfully 6745B8E0. *May 4 00:44:20.985: ISAKMP: set new node 1361385973 to CONF_XAUTH *May 4 00:44:20.985: ISAKMP:(1008):Sending NOTIFY RESPONDER_LIFETIME protocol 1 spi 1722618680, message ID = 1361385973 *May 4 00:44:20.985: ISAKMP:(1008): sending packet to 172.16.186.130 my_port 500 peer_port 500 (R) QM_IDLE *May 4 00:44:20.985: ISAKMP:(1008):purging node 1361385973 *May 4 00:44:20.985: ISAKMP: Sending phase 1 responder lifetime 86400 *May 4 00:44:20.985: ISAKMP:(1008):Input = IKE_MSG_FROM_PEER, IKE_AM_EXCH *May 4 00:44:20.985: ISAKMP:(1008):Old State = IKE_R_AM2 New State = **IKE_P1_COMPLETE** !--- Requesting Xauth. *May 4 00:44:20.985: IPSEC(key_engine): got a queue event with 1 KMI message(s) *May 4 00:44:20.985: ISAKMP:(1008):Need XAUTH *May 4 00:44:20.985: ISAKMP: set new node -605466681 to CONF_XAUTH *May 4 00:44:20.985: ISAKMP/xauth: request attribute XAUTH_USER_NAME_V2 *May 4 00:44:20.985: ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD_V2 *May 4 00:44:20.985: ISAKMP:(1008): initiating peer config to 172.16.186.130. ID = -605466681 *May 4 00:44:20.985: ISAKMP:(1008): sending packet to 172.16.186.130 my_port 500 peer_port 500 (R) CONF_XAUTH *May 4 00:44:20.985: ISAKMP:(1008):Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE *May 4 00:44:20.985: ISAKMP:(1008):Old State = IKE_P1_COMPLETE New State = IKE_XAUTH_REQ_SENT *May 4 00:44:35.985: ISAKMP:(1008): retransmitting phase 2 CONF_XAUTH -605466681 ... *May 4 00:44:35.985: ISAKMP (0:1008): incrementing error counter on node, attempt 1 of 5: retransmit phase 2 *May 4 00:44:35.985: ISAKMP (0:1008): incrementing error counter on sa, attempt 1 of 5: retransmit phase 2 *May 4 00:44:35.985: ISAKMP:(1008): retransmitting phase 2 -605466681 CONF_XAUTH *May 4 00:44:35.985: ISAKMP:(1008): sending packet to 172.16.186.130 my_port 500 peer_port 500 (R) CONF_XAUTH R# 3-07-07-7200VXR# *May 4 00:44:50.985: ISAKMP:(1008): retransmitting phase 2 CONF_XAUTH -605466681 ... *May 4 00:44:50.985: ISAKMP (0:1008): incrementing error counter on node, attempt 2 of 5: retransmit phase 2 *May 4 00:44:50.985: ISAKMP (0:1008): incrementing error counter on sa, attempt 2 of 5: retransmit phase 2 *May 4 00:44:50.985: ISAKMP:(1008): retransmitting phase 2 -605466681 CONF_XAUTH *May 4 00:44:50.985: ISAKMP:(1008): sending packet to 172.16.186.130 my_port 500 peer_port 500 (R) CONF_XAUTH 3-07-07-7200VXR# *May 4 00:45:01.997: ISAKMP (0:1008): received packet from 172.16.186.130 dport 500 sport 500 Global (R) CONF_XAUTH *May 4 00:45:01.997: ISAKMP:(1008):processing transaction payload from 172.16.186.130. message ID = -605466681 *May 4 00:45:01.997: ISAKMP: Config payload REPLY *May 4 00:45:01.997: ISAKMP/xauth: reply attribute XAUTH_USER_NAME_V2 *May 4 00:45:01.997: ISAKMP/xauth: reply attribute XAUTH_USER_PASSWORD_V2 *May 4 00:45:01.997: ISAKMP:(1008):deleting node -605466681 error FALSE reason "Done with xauth request/reply exchange" *May 4 00:45:01.997: ISAKMP:(1008):Input = IKE_MSG_FROM_PEER, IKE_CFG_REPLY *May 4 00:45:01.997: ISAKMP:(1008):Old State = IKE_XAUTH_REQ_SENT New State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT *May 4 00:45:01.997: ISAKMP: set new node 1283697340 to CONF_XAUTH *May 4 00:45:01.997: ISAKMP:(1008): initiating peer config to 172.16.186.130. ID = 1283697340 *May 4 00:45:01.997: ISAKMP:(1008): sending packet to 172.16.186.130 my_port 5 3-07-07-7200VX00 peer_port 500 (R) CONF_XAUTH *May 4 00:45:01.997: ISAKMP:(1008):Input = IKE_MSG_FROM_AAA, IKE_AAA_CONT_LOGIN *May 4 00:45:01.997: ISAKMP:(1008):Old State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT New State = IKE_XAUTH_SET_SENT *May 4 00:45:02.005: ISAKMP (0:1008): received packet from 172.16.186.130 dport 500 sport 500 Global (R) CONF_XAUTH *May 4 00:45:02.005: ISAKMP:(1008):processing transaction payload from 172.16.186.130. message ID = 1283697340 *May 4 00:45:02.005: ISAKMP: Config payload ACK *May 4 00:45:02.005: ISAKMP:(1008): XAUTH ACK Processed *May 4 00:45:02.005: ISAKMP:(1008):deleting node 1283697340 error FALSE reason "Transaction mode done" *May 4 00:45:02.005: ISAKMP:(1008):Input = IKE_MSG_FROM_PEER, IKE_CFG_ACK *May 4 00:45:02.005: ISAKMP:(1008):Old State = IKE_XAUTH_SET_SENT New State = IKE_P1_COMPLETE *May 4 00:45:02.005: ISAKMP:(1008):Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE *May 4 00:45:02.005: ISAKMP:(1008):Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE *May 4 00:45:02.005: ISAKMP (0:1008): received packet from 172.16.186.130 dport 500 sport 500 Global (R) QM_IDLE *May 4 00:45:02.005: ISAKMP: set new node 104696831 to QM_IDLE *May 4 00:45:02.005: ISAKMP:(1008):processing transaction payload from 172.16.186.130. message ID = 104696831 *May 4 00:45:02.005: ISAKMP: Config payload REQUEST *May 4 00:45:02.005: ISAKMP:(1008):checking request: *May 4 00:45:02.005: ISAKMP: MODECFG_CONFIG_URL *May 4 00:45:02.005: ISAKMP: MODECFG_CONFIG_VERSION *May 4 00:45:02.009: ISAKMP: IP4_DNS *May 4 00:45:02.009: ISAKMP: IP4_DNS *May 4 00:45:02.009: ISAKMP: IP4_NBNS *May 4 00:45:02.009: ISAKMP: IP4_NBNS *May 4 00:45:02.009: ISAKMP: SPLIT_INCLUDE *May 4 00:45:02.009: ISAKMP: SPLIT_DNS *May 4 00:45:02.009: ISAKMP: DEFAULT_DOMAIN *May 4 00:45:02.009: ISAKMP: MODECFG_SAVEPWD *May 4 00:45:02.009: ISAKMP: INCLUDE_LOCAL_LAN *May 4 00:45:02.009: ISAKMP: PFS *May 4 00:45:02.009: ISAKMP: BACKUP_SERVER *May 4 00:45:02.009: ISAKMP: APPLICATION_VERSION *May 4 00:45:02.009: ISAKMP: MODECFG-BANNER *May 4 00:45:02.009: ISAKMP: MODECFG_IPSEC_INT_CONF *May

4 00:45:02.009: ISAKMP/author: Author request for group vpngrpssuccessfully sent to AAA *May 4
00:45:02.009: ISAKMP:(1008):Input = IKE_MSG_FROM_PEER, IKE_CFG_REQUEST *May 4 00:45:02.009:
ISAKMP:(1008):Old State = IKE_P1_COMPLETE New State = IKE_CONFIG_AUTHOR_AAA_AWAIT *May 4
00:45:02.009: ISAKMP:(1008):Receive config attributes requested butconfig attributes not in
crypto map. Sending empty reply. *May 4 00:45:02.009: ISAKMP:(1008):attributes sent in message:
*May 4 00:45:02.009: ISAKMP: Sending APPLICATION_VERSION string: Cisco IOS Software, 7200
Software (C7200-ADVENTERPRISEK9-M), Version 12.4(4)T1, RELEASE SOFTWARE (fc4) Technical Support:
http://www.cisco.com/techsupport Copyright (c) 1986-2005 by Cisco Systems, Inc. Compiled Wed 21-
Dec-05 22:58 by ccai *May 4 00:45:02.009: ISAKMP: Sending IPsec Interface Config reply value 0
*May 4 00:45:02.009: ISAKMP:(1008): responding to peer config from 172.16.186.130. ID =
104696831 *May 4 00:45:02.009: ISAKMP:(1008): sending packet to 172.16.186.130 my_port 500
peer_port 500 (R) CONF_ADDR *May 4 00:45:02.009: ISAKMP:(1008):deleting node 104696831 error
FALSE reason "No Error" *May 4 00:45:02.009: ISAKMP:(1008):Input = IKE_MSG_FROM_AAA,
IKE_AAA_GROUP_ATTR *May 4 00:45:02.009: ISAKMP:(1008):Old State = IKE_CONFIG_AUTHOR_AAA_AWAIT
New State = IKE_P1_COMPLETE *May 4 00:45:02.009: ISAKMP:(1008):Input = IKE_MSG_INTERNAL,
IKE_PHASE1_COMPLETE *May 4 00:45:02.009: ISAKMP:(1008):Old State = IKE_P1_COMPLETE New State =
IKE_P1_COMPLETE *May 4 00:45:02.029: ISAKMP (0:1008): received packet from 172.16.186.130 dport
500 sport 500 Global (R) QM_IDLE *May 4 00:45:02.029: ISAKMP: set new node -1665883002 to
QM_IDLE *May 4 00:45:02.029: ISAKMP:(1008): processing HASH payload. message ID = -1665883002
*May 4 00:45:02.029: ISAKMP:(1008): processing SA payload. message ID = -1665883002 *May 4
00:45:02.029: ISAKMP:(1008):Checking IPsec proposal 1 *May 4 00:45:02.029: ISAKMP: transform 1,
ESP_AES *May 4 00:45:02.029: ISAKMP: attributes in transform: *May 4 00:45:02.029: ISAKMP:
encaps is 1 (Tunnel) *May 4 00:45:02.029: ISAKMP: SA life type in seconds *May 4 00:45:02.029:
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B *May 4 00:45:02.029: ISAKMP: SA life type
in kilobytes *May 4 00:45:02.029: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 *May 4
00:45:02.029: ISAKMP: authenticator is HMAC-SHA *May 4 00:45:02.029: ISAKMP: key length is 128
*May 4 00:45:02.029: ISAKMP:(1008):atts are acceptable. *May 4 00:45:02.029:
IPSEC(validate_proposal_request): proposal part #1 *May 4 00:45:02.029:
IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local=
172.16.186.186, remote= 172.16.186.130, local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), remote_proxy=
10.12.130.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-aes esp-sha-hmac
(Tunnel), lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0 *May 4
00:45:02.029: IPSEC(crypto_ipsec_process_proposal): transform proposal not supported for
identity: {esp-aes esp-sha-hmac } *May 4 00:45:02.029: ISAKMP:(1008): IPsec policy invalidated
proposal *May 4 00:45:02.029: ISAKMP:(1008):Checking IPsec proposal 2 *May 4 00:45:02.029:
ISAKMP: transform 1, ESP_AES *May 4 00:45:02.029: ISAKMP: attributes in transform: *May 4
00:45:02.029: ISAKMP: encaps is 1 (Tunnel) *May 4 00:45:02.029: ISAKMP: SA life type in seconds
*May 4 00:45:02.029: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B *May 4 00:45:02.029:
ISAKMP: SA life type in kilobytes *May 4 00:45:02.029: ISAKMP: SA life duration (VPI) of 0x0
0x46 0x50 0x0 *May 4 00:45:02.029: ISAKMP: authenticator is HMAC-MD5 *May 4 00:45:02.029:
ISAKMP: key length is 128 *May 4 00:45:02.029: ISAKMP:(1008):atts are acceptable. *May 4
00:45:02.029: IPSEC(validate_proposal_request): proposal part #1 *May 4 00:45:02.029:
IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local=
172.16.186.186, remote= 172.16.186.130, local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), remote_proxy=
10.12.130.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-aes esp-md5-hmac
(Tunnel), lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0 *May 4
00:45:02.029: IPSEC(crypto_ipsec_process_proposal): transform proposal not supported for
identity: {esp-aes esp-md5-hmac } *May 4 00:45:02.029: ISAKMP:(1008): IPsec policy invalidated
proposal *May 4 00:45:02.029: ISAKMP:(1008):Checking IPsec proposal 3 *May 4 00:45:02.029:
ISAKMP: transform 1, ESP_AES *May 4 00:45:02.029: ISAKMP: attributes in transform: *May 4
00:45:02.029: ISAKMP: encaps is 1 (Tunnel) *May 4 00:45:02.029: ISAKMP: SA life type in seconds
*May 4 00:45:02.029: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B *May 4 00:45:02.029:
ISAKMP: SA life type in kilobytes *May 4 00:45:02.029: ISAKMP: SA life duration (VPI) of 0x0
0x46 0x50 0x0 *May 4 00:45:02.029: ISAKMP: authenticator is HMAC-SHA *May 4 00:45:02.029:
ISAKMP: key length is 192 *May 4 00:45:02.029: ISAKMP:(1008):atts are acceptable. *May 4
00:45:02.029: IPSEC(validate_proposal_request): proposal part #1 *May 4 00:45:02.029:
IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local=
172.16.186.186, remote= 172.16.186.130, local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), remote_proxy=
10.12.130.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-aes 192 esp-sha-hmac
(Tunnel), lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 192, flags= 0x0 *May 4
00:45:02.029: IPSEC(crypto_ipsec_process_proposal): transform proposal not supported for
identity: {esp-aes 192 esp-sha-hmac } *May 4 00:45:02.029: ISAKMP:(1008): IPsec policy
invalidated proposal *May 4 00:45:02.029: ISAKMP:(1008):Checking IPsec proposal 4 *May 4
00:45:02.029: ISAKMP: transform 1, ESP_AES *May 4 00:45:02.029: ISAKMP: attributes in transform:

*May 4 00:45:02.029: ISAKMP: encaps is 1 (Tunnel) *May 4 00:45:02.029: ISAKMP: SA life type in seconds *May 4 00:45:02.029: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9B *May 4 00:45:02.029: ISAKMP: SA life type in kilobytes *May 4 00:45:02.029: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 *May 4 00:45:02.029: ISAKMP: authenticator is HMAC-MD5 *May 4 00:45:02.029: ISAKMP: key length is 192 *May 4 00:45:02.029: ISAKMP:(1008):atts are acceptable. *May 4 00:45:02.029: IPSEC(validate_proposal_request): proposal part #1 *May 4 00:45:02.029: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local=172.16.186.186, remote= 172.16.186.130, local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), remote_proxy=10.12.130.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-aes 192 esp-md5-hmac (Tunnel), lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 192, flags= 0x0 *May 4 00:45:02.029: IPSEC(crypto_ipsec_process_proposal): transform proposal not supported for identity: {esp-aes 192 esp-md5-hmac } *May 4 00:45:02.029: ISAKMP:(1008): IPsec policy invalidated proposal *May 4 00:45:02.029: ISAKMP:(1008):Checking IPsec proposal 5 *May 4 00:45:02.029: ISAKMP: transform 1, ESP_AES *May 4 00:45:02.029: ISAKMP: attributes in transform: *May 4 00:45:02.029: ISAKMP: encaps is 1 (Tunnel) *May 4 00:45:02.029: ISAKMP: SA life type in seconds *May 4 00:45:02.029: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9B *May 4 00:45:02.029: ISAKMP: SA life type in kilobytes *May 4 00:45:02.029: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 *May 4 00:45:02.029: ISAKMP: authenticator is HMAC-SHA *May 4 00:45:02.033: ISAKMP: key length is 256 *May 4 00:45:02.033: ISAKMP:(1008):atts are acceptable. *May 4 00:45:02.033: IPSEC(validate_proposal_request): proposal part #1 *May 4 00:45:02.033: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local=172.16.186.186, remote= 172.16.186.130, local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), remote_proxy=10.12.130.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-aes 256 esp-sha-hmac (Tunnel), lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x0 *May 4 00:45:02.033: IPSEC(crypto_ipsec_process_proposal): transform proposal not supported for identity: {esp-aes 256 esp-sha-hmac } *May 4 00:45:02.033: ISAKMP:(1008): IPsec policy invalidated proposal *May 4 00:45:02.033: ISAKMP:(1008):Checking IPsec proposal 6 *May 4 00:45:02.033: ISAKMP: transform 1, ESP_AES *May 4 00:45:02.033: ISAKMP: attributes in transform: *May 4 00:45:02.033: ISAKMP: encaps is 1 (Tunnel) *May 4 00:45:02.033: ISAKMP: SA life type in seconds *May 4 00:45:02.033: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9B *May 4 00:45:02.033: ISAKMP: SA life type in kilobytes *May 4 00:45:02.033: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 *May 4 00:45:02.033: ISAKMP: authenticator is HMAC-MD5 *May 4 00:45:02.033: ISAKMP: key length is 256 *May 4 00:45:02.033: ISAKMP:(1008):atts are acceptable. *May 4 00:45:02.033: IPSEC(validate_proposal_request): proposal part #1 *May 4 00:45:02.033: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local=172.16.186.186, remote= 172.16.186.130, local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), remote_proxy=10.12.130.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-aes 256 esp-md5-hmac (Tunnel), lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x0 *May 4 00:45:02.033: IPSEC(crypto_ipsec_process_proposal): transform proposal not supported for identity: {esp-aes 256 esp-md5-hmac } *May 4 00:45:02.033: ISAKMP:(1008): IPsec policy invalidated proposal *May 4 00:45:02.033: ISAKMP:(1008):Checking IPsec proposal 7 *May 4 00:45:02.033: ISAKMP: transform 1, ESP_3DES *May 4 00:45:02.033: ISAKMP: attributes in transform: *May 4 00:45:02.033: ISAKMP: encaps is 1 (Tunnel) *May 4 00:45:02.033: ISAKMP: SA life type in seconds *May 4 00:45:02.033: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9B *May 4 00:45:02.033: ISAKMP: SA life type in kilobytes *May 4 00:45:02.033: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 *May 4 00:45:02.033: ISAKMP: authenticator is HMAC-SHA *May 4 00:45:02.033: ISAKMP:(1008):atts are acceptable. *May 4 00:45:02.033: IPSEC(validate_proposal_request): proposal part #1 *May 4 00:45:02.033: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local=172.16.186.186, remote= 172.16.186.130, local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), remote_proxy=10.12.130.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-3des esp-sha-hmac (Tunnel), lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0 *May 4 00:45:02.033: ISAKMP:(1008): processing NONCE payload. message ID = -1665883002 *May 4 00:45:02.033: ISAKMP:(1008): processing ID payload. message ID = -1665883002 *May 4 00:45:02.033: ISAKMP:(1008): processing ID payload. message ID = -1665883002 *May 4 00:45:02.033: ISAKMP:(1008): asking for 1 spis from ipsec *May 4 00:45:02.033: ISAKMP:(1008):Node -1665883002, Input = IKE_MSG_FROM_PEER, IKE_QM_EXCH *May 4 00:45:02.033: ISAKMP:(1008):Old State = IKE_QM_READY New State = IKE_QM_SPI_STARVE *May 4 00:45:02.033: IPSEC(key_engine): got a queue event with 1 KMI message(s) *May 4 00:45:02.033: IPSEC(spi_response): getting spi 1752561220 for SA from 172.16.186.186 to 172.16.186.130 for prot 3 *May 4 00:45:02.033: ISAKMP:(1008): Creating IPsec SAs *May 4 00:45:02.033: inbound SA from 172.16.186.130 to 172.16.186.186 (f/i) 0/ 0 (proxy 10.12.130.1 to 0.0.0.0) *May 4 00:45:02.033: has spi 0x6875F644 and conn_id 0 *May 4 00:45:02.033: lifetime of 2147483 seconds *May 4 00:45:02.033: lifetime of 4608000 kilobytes *May 4 00:45:02.033: outbound SA from

```

172.16.186.186 to 172.16.186.130 (f/i) 0/0 (proxy 0.0.0.0 to 10.12.130.1) *May 4 00:45:02.033:
has spi 0x29354010 and conn_id 0 *May 4 00:45:02.033: lifetime of 2147483 seconds *May 4
00:45:02.033: lifetime of 4608000 kilobytes *May 4 00:45:02.033: ISAKMP:(1008): sending packet
to 172.16.186.130 my_port 500 peer_port 500 (R) QM_IDLE *May 4 00:45:02.033: ISAKMP:(1008):Node
-1665883002, Input = IKE_MSG_FROM_IPSEC, IKE_SPI_REPLY *May 4 00:45:02.033: ISAKMP:(1008):Old
State = IKE_QM_SPI_STARVE New State = IKE_QM_R_QM2 *May 4 00:45:02.033: IPSEC(key_engine): got a
queue event with 1 KMI message(s) *May 4 00:45:02.033: IPsec: Flow_switching Allocated flow for
sibling 80000007 *May 4 00:45:02.033: IPSEC(policy_db_add_ident): src 0.0.0.0, dest 10.12.130.1,
dest_port 0 *May 4 00:45:02.033: IPSEC(create_sa): sa created, (sa) sa_dest= 172.16.186.186,
sa_proto= 50, sa_spi= 0x6875F644(1752561220), sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 11
*May 4 00:45:02.033: IPSEC(create_sa): sa created, (sa) sa_dest= 172.16.186.130, sa_proto= 50,
sa_spi= 0x29354010(691355664), sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 12 *May 4
00:45:02.045: ISAKMP (0:1008): received packet from 172.16.186.130 dport 500 sport 500 Global
(R) QM_IDLE *May 4 00:45:02.045: ISAKMP:(1008):deleting node -1665883002 error FALSE reason "QM
done (await)" *May 4 00:45:02.045: ISAKMP:(1008):Node -1665883002, Input = IKE_MSG_FROM_PEER,
IKE_QM_EXCH *May 4 00:45:02.045: ISAKMP:(1008):Old State = IKE_QM_R_QM2 New State =
IKE_QM_PHASE2_COMPLETE *May 4 00:45:02.045: IPSEC(key_engine): got a queue event with 1 KMI
message(s) *May 4 00:45:02.045: IPSEC(key_engine_enable_outbound): rec'd enable notify from
ISAKMP *May 4 00:45:02.045: IPSEC(key_engine_enable_outbound): enable SA with spi 691355664/50

```

Easy VPN リモートのコマンド

- **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表示します。

```

3-03-06-871W#debug crypto ipsec3-03-06-871W#debug crypto isakmp
*Jun  3 05:59:27.431: ISAKMP:(0): beginning Aggressive Mode exchange
*Jun  3 05:59:27.431: ISAKMP:(0): sending packet to 172.16.186.186 my_port
      500 peer_port 500 (I) AG_INIT_EXCH
*Jun  3 05:59:27.455: ISAKMP (0:0): received packet from 172.16.186.186 dport
      500 sport 500 Global (I) AG_INIT_EXCH
*Jun  3 05:59:27.455: ISAKMP:(0): processing SA payload. message ID = 0
*Jun  3 05:59:27.455: ISAKMP:(0): processing ID payload. message ID = 0
*Jun  3 05:59:27.455: ISAKMP (0:0): ID payload
      next-payload : 10
      type          : 1
      address       : 172.16.186.186
      protocol      : 17
      port          : 0
      length        : 12
*Jun  3 05:59:27.455: ISAKMP:(0):: peer matches *none* of the profiles
*Jun  3 05:59:27.455: ISAKMP:(0): processing vendor id payload
*Jun  3 05:59:27.455: ISAKMP:(0): vendor ID is Unity
*Jun  3 05:59:27.455: ISAKMP:(0): processing vendor id payload
*Jun  3 05:59:27.455: ISAKMP:(0): vendor ID is DPD
*Jun  3 05:59:27.455: ISAKMP:(0): processing vendor id payload
*Jun  3 05:59:27.455: ISAKMP:(0): speaking to another IOS box!
*Jun  3 05:59:27.455: ISAKMP:(0): local preshared key found
*Jun  3 05:59:27.455: ISAKMP : Scanning profiles for xauth ...
*Jun  3 05:59:27.455: ISAKMP:(0): Authentication by xauth preshared
*Jun  3 05:59:27.455: ISAKMP:(0):Checking ISAKMP transform 1 against priority 65515 policy
*Jun  3 05:59:27.455: ISAKMP:      encryption 3DES-CBC
*Jun  3 05:59:27.455: ISAKMP:      hash SHA
*Jun  3 05:59:27.455: ISAKMP:      default group 2
*Jun  3 05:59:27.459: ISAKMP:      auth XAUTHInitPreShared
*Jun  3 05:59:27.459: ISAKMP:      life type in seconds
*Jun  3 05:59:27.459: ISAKMP:      life duration (VPI) of  0x0 0x20 0xC4 0x9B
*Jun  3 05:59:27.459: ISAKMP:(0):Encryption algorithm offered does not match policy!
*Jun  3 05:59:27.459: ISAKMP:(0):atts are not acceptable. Next payload is 0
*Jun  3 05:59:27.459: ISAKMP:(0):Checking ISAKMP transform 1 against priority 65516 policy
*Jun  3 05:59:27.459: ISAKMP:      encryption 3DES-CBC
*Jun  3 05:59:27.459: ISAKMP:      hash SHA
*Jun  3 05:59:27.459: ISAKMP:      default group 2

```


*Jun 3 05:59:27.463: ISAKMP: life type in seconds
*Jun 3 05:59:27.463: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
*Jun 3 05:59:27.463: ISAKMP:(0):Encryption algorithm offered does not match policy!
*Jun 3 05:59:27.463: ISAKMP:(0):atts are not acceptable. Next payload is 0
*Jun 3 05:59:27.463: ISAKMP:(0):Checking ISAKMP transform 1 against priority 65524 policy
*Jun 3 05:59:27.467: ISAKMP: encryption 3DES-CBC
*Jun 3 05:59:27.467: ISAKMP: hash SHA
*Jun 3 05:59:27.467: ISAKMP: default group 2
*Jun 3 05:59:27.467: ISAKMP: auth XAUTHInitPreShared
*Jun 3 05:59:27.467: ISAKMP: life type in seconds
*Jun 3 05:59:27.467: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
*Jun 3 05:59:27.467: ISAKMP:(0):Encryption algorithm offered does not match policy!
*Jun 3 05:59:27.467: ISAKMP:(0):atts are not acceptable. Next payload is 0
*Jun 3 05:59:27.467: ISAKMP:(0):Checking ISAKMP transform 1 against priority 65525 policy
*Jun 3 05:59:27.467: ISAKMP: encryption 3DES-CBC
*Jun 3 05:59:27.467: ISAKMP: hash SHA
*Jun 3 05:59:27.467: ISAKMP: default group 2
*Jun 3 05:59:27.467: ISAKMP: auth XAUTHInitPreShared
*Jun 3 05:59:27.467: ISAKMP: life type in seconds
*Jun 3 05:59:27.467: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
*Jun 3 05:59:27.467: ISAKMP:(0):Encryption algorithm offered does not match policy!
*Jun 3 05:59:27.467: ISAKMP:(0):atts are not acceptable. Next payload is 0
*Jun 3 05:59:27.467: ISAKMP:(0):Checking ISAKMP transform 1 against priority 65526 policy
*Jun 3 05:59:27.467: ISAKMP: encryption 3DES-CBC
*Jun 3 05:59:27.467: ISAKMP: hash SHA
*Jun 3 05:59:27.467: ISAKMP: default group 2
*Jun 3 05:59:27.467: ISAKMP: auth XAUTHInitPreShared
*Jun 3 05:59:27.467: ISAKMP: life type in seconds
*Jun 3 05:59:27.467: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
*Jun 3 05:59:27.467: ISAKMP:(0):Encryption algorithm offered does not match policy!
*Jun 3 05:59:27.467: ISAKMP:(0):atts are not acceptable. Next payload is 0
*Jun 3 05:59:27.467: ISAKMP:(0):Checking ISAKMP transform 1 against priority 65527 policy
*Jun 3 05:59:27.467: ISAKMP: encryption 3DES-CBC
*Jun 3 05:59:27.467: ISAKMP: hash SHA
*Jun 3 05:59:27.467: ISAKMP: default group 2
*Jun 3 05:59:27.467: ISAKMP: auth XAUTHInitPreShared
*Jun 3 05:59:27.467: ISAKMP: life type in seconds
*Jun 3 05:59:27.467: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
*Jun 3 05:59:27.467: ISAKMP:(0):atts are acceptable. Next payload is 0 *Jun 3 05:59:27.467:
ISAKMP (0:0): vendor ID is NAT-T v7 *Jun 3 05:59:27.467: ISAKMP:(0): processing KE payload.
message ID = 0 *Jun 3 05:59:27.475: ISAKMP:(0): processing NONCE payload. message ID = 0 *Jun 3
05:59:27.475: ISAKMP:(2006): processing HASH payload. message ID = 0 *Jun 3 05:59:27.475:
ISAKMP:(2006):SA authentication status: authenticated *Jun 3 05:59:27.475: ISAKMP:(2006):SA has
been authenticated with 172.16.186.186 *Jun 3 05:59:27.475: ISAKMP:(2006):Send initial contact
*Jun 3 05:59:27.475: ISAKMP:(2006): sending packet to 172.16.186.186 my_port 500 peer_port 500
(I) AG_INIT_EXCH *Jun 3 05:59:27.479: ISAKMP:(2006):Input = IKE_MSG_FROM_PEER, IKE_AM_EXCH *Jun
3 05:59:27.479: ISAKMP:(2006):Old State = IKE_I_AM1 New State = IKE_P1_COMPLETE *Jun 3
05:59:27.479: ISAKMP:(2006):Need XAUTH *Jun 3 05:59:27.479: ISAKMP:(2006):Input =
IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE **!--- Phase 1 (ISAKMP) is complete.** *Jun 3 05:59:27.479:
ISAKMP:(2006):Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE **!--- Xauth initiates.** *Jun
3 05:59:27.479: ISAKMP (0:2006): received packet from 172.16.186.186 dport 500 sport 500 Global
(I) CONF_XAUTH *Jun 3 05:59:27.483: ISAKMP: set new node 850198625 to CONF_XAUTH *Jun 3
05:59:27.487: ISAKMP:(2006):processing transaction payload from 172.16.186.186. message ID = -
1517216966 *Jun 3 05:59:27.487: ISAKMP: Config payload REQUEST *Jun 3 05:59:27.487:
ISAKMP:(2006):checking request: *Jun 3 05:59:27.487: ISAKMP: XAUTH_USER_NAME_V2 *Jun 3
05:59:27.487: ISAKMP: XAUTH_USER_PASSWORD_V2 *Jun 3 05:59:27.487: ISAKMP:(2006):Xauth process
request *Jun 3 05:59:27.487: ISAKMP:(2006):Input = IKE_MSG_FROM_PEER, IKE_CFG_REQUEST *Jun 3
05:59:27.487: ISAKMP:(2006):Old State = IKE_P1_COMPLETE New State = IKE_XAUTH_REPLY_AWAIT *Jun 3
05:59:30.242: EZVPN(ez): Pending XAuth Request, Please enter the following command: *Jun 3
05:59:30.242: EZVPN: crypto ipsec client ezvpn xauth **!--- Enter the crypto ipsec client ezvpn
xauth command.** 3-03-06-871W#crypto ipsec client ezvpn xauth Username: cisco Password: <omitted>
*Jun 3 06:02:46.498: username: cisco *Jun 3 06:02:46.498: password: <omitted> *Jun 3
06:02:46.498: ISAKMP:(2008): responding to peer config from 172.16.186.186. ID = -605466681 *Jun
3 06:02:46.498: ISAKMP:(2008): sending packet to 172.16.186.186 my_port 500 peer_port 500 (I)

CONF_XAUTH *Jun 3 06:02:46.498: ISAKMP:(2008):deleting node -605466681 error FALSE reason "Done with xauth request/reply exchange" *Jun 3 06:02:46.498: ISAKMP:(2008):Input = IKE_MSG_INTERNAL, IKE_XAUTH_REPLY_ATTR *Jun 3 06:02:46.498: ISAKMP:(2008):Old State = IKE_XAUTH_REPLY_AWAIT New State = IKE_XAUTH_REPLY_SENT *Jun 3 06:02:46.502: ISAKMP (0:2008): received packet from 172.16.186.186 dport 500 sport 500 Global (I) CONF_XAUTH *Jun 3 06:02:46.502: ISAKMP: set new node 1283697340 to CONF_XAUTH *Jun 3 06:02:46.502: ISAKMP:(2008):processing transaction payload from 172.16.186.186. message ID = 1283697340 *Jun 3 06:02:46.502: ISAKMP: Config payload SET *Jun 3 06:02:46.502: ISAKMP:(2008):Xauth process set, status = 1 *Jun 3 06:02:46.502: ISAKMP:(2008):checking SET: *Jun 3 06:02:46.502: ISAKMP: XAUTH_STATUS_V2 XAUTH-OK *Jun 3 06:02:46.502: ISAKMP:(2008):attributes sent in message: *Jun 3 06:02:46.502: Status: 1 *Jun 3 06:02:46.506: ISAKMP:(2008): sending packet to 172.16.186.186 my_port 500 peer_port 500 (I) CONF_XAUTH *Jun 3 06:02:46.506: ISAKMP:(2008):deleting node 1283697340 error FALSE reason "No Error" *Jun 3 06:02:46.506: ISAKMP:(2008):Input = IKE_MSG_FROM_PEER, IKE_CFG_SET *Jun 3 06:02:46.506: ISAKMP:(2008):Old State = IKE_XAUTH_REPLY_SENT New State = IKE_P1_COMPLETE *Jun 3 06:02:46.506: ISAKMP:(2008):Need config/address *Jun 3 06:02:46.506: ISAKMP: set new node 104696831 to CONF_ADDR *Jun 3 06:02:46.506: ISAKMP: Sending APPLICATION_VERSION string: Cisco IOS Software, C870 Software (C870-ADVIPSERVICESK9-M), Experimental Version 12.4(20060201:210845) [prchadal-CSCsb79792-haw_t_pi4 101] Copyright (c) 1986-2006 by Cisco Systems, Inc. Compiled Thu 02-Feb-06 03:19 by prchadal *Jun 3 06:02:46.506: ISAKMP:(2008): initiating peer config to 172.16.186.186. ID = 104696831 *Jun 3 06:02:46.506: ISAKMP:(2008): sending packet to 172.16.186.186 my_port 500 peer_port 500 (I) CONF_ADDR *Jun 3 06:02:46.506: ISAKMP:(2008):Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE *Jun 3 06:02:46.506: ISAKMP:(2008):Old State = IKE_P1_COMPLETE New State = IKE_CONFIG_MODE_REQ_SENT *Jun 3 06:02:46.510: ISAKMP (0:2008): received packet from 172.16.186.186 dport 500 sport 500 Global (I) CONF_ADDR *Jun 3 06:02:46.514: ISAKMP:(2008):processing transaction payload from 172.16.186.186. message ID = 104696831 *Jun 3 06:02:46.514: ISAKMP: Config payload REPLY *Jun 3 06:02:46.514: ISAKMP(0:2008) process config reply *Jun 3 06:02:46.514: ISAKMP:(2008):deleting node 104696831 error FALSE reason "Transaction mode done" *Jun 3 06:02:46.514: ISAKMP:(2008):Input = IKE_MSG_FROM_PEER, IKE_CFG_REPLY *Jun 3 06:02:46.514: ISAKMP:(2008):Old State = IKE_CONFIG_MODE_REQ_SENT New State = IKE_P1_COMPLETE *Jun 3 06:02:46.518: insert of map into mapdb AVL failed, map + ace pair already exists on the mapdb *Jun 3 06:02:46.518: ISAKMP:(2008):Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE *Jun 3 06:02:46.518: ISAKMP:(2008):Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE *Jun 3 06:02:46.522: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.186.130, remote= 172.16.186.186, local_proxy= 10.12.130.1/255.255.255.255/0/0 (type=1), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= NONE (Tunnel), lifedur= 2147483s and 4608000kb, spi= 0xA0FC0985(2700872069), conn_id= 0, keysize= 128, flags= 0x2000 *Jun 3 06:02:46.522: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.186.130, remote= 172.16.186.186, local_proxy= 10.12.130.1/255.255.255.255/0/0 (type=1), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= NONE (Tunnel), lifedur= 2147483s and 4608000kb, spi= 0xBB426C9(196355785), conn_id= 0, keysize= 128, flags= 0x2000 *Jun 3 06:02:46.522: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.186.130, remote= 172.16.186.186, local_proxy= 10.12.130.1/255.255.255.255/0/0 (type=1), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= NONE (Tunnel), lifedur= 2147483s and 4608000kb, spi= 0xB349BB06(3007953670), conn_id= 0, keysize= 192, flags= 0x2000 *Jun 3 06:02:46.522: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.186.130, remote= 172.16.186.186, local_proxy= 10.12.130.1/255.255.255.255/0/0 (type=1), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= NONE (Tunnel), lifedur= 2147483s and 4608000kb, spi= 0xC114CFB8(3239366584), conn_id= 0, keysize= 192, flags= 0x2000 *Jun 3 06:02:46.522: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.186.130, remote= 172.16.186.186, local_proxy= 10.12.130.1/255.255.255.255/0/0 (type=1), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= NONE (Tunnel), lifedur= 2147483s and 4608000kb, spi= 0x2ED87C62(785939554), conn_id= 0, keysize= 256, flags= 0x2000 *Jun 3 06:02:46.522: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.186.130, remote= 172.16.186.186, local_proxy= 10.12.130.1/255.255.255.255/0/0 (type=1), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= NONE (Tunnel), lifedur= 2147483s and 4608000kb, spi= 0x226A6FF3(577400819), conn_id= 0, keysize= 256, flags= 0x2000 *Jun 3 06:02:46.522: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.186.130, remote= 172.16.186.186, local_proxy= 10.12.130.1/255.255.255.255/0/0 (type=1), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= NONE (Tunnel), lifedur= 2147483s and 4608000kb, spi= 0x29354010(691355664), conn_id= 0, keysize= 0, flags= 0x2000 *Jun 3 06:02:46.526: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.186.130, remote= 172.16.186.186, local_proxy= 10.12.130.1/255.255.255.255/0/0 (type=1), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= NONE (Tunnel), lifedur= 2147483s and 4608000kb, spi= 0x12111E5C(303111772), conn_id= 0, keysize= 0, flags= 0x2000 *Jun 3

06:02:46.526: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.186.130, remote= 172.16.186.186, local_proxy= 10.12.130.1/255.255.255.255/0/0 (type=1), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= NONE (Tunnel), lifedur= 2147483s and 4608000kb, spi= 0x98084B9A(2550680474), conn_id= 0, keysize= 0, flags= 0x2000 *Jun 3
06:02:46.526: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.186.130, remote= 172.16.186.186, local_proxy= 10.12.130.1/255.255.255.255/0/0 (type=1), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= NONE (Tunnel), lifedur= 2147483s and 4608000kb, spi= 0x9442501B(2487373851), conn_id= 0, keysize= 0, flags= 0x0 *Jun 3
06:02:46.526: ISAKMP: set new node 0 to QM_IDLE *Jun 3 06:02:46.526: ISAKMP:(2008): sitting IDLE. Starting QM immediately (QM_IDLE) *Jun 3 06:02:46.526: ISAKMP:(2008):beginning Quick Mode exchange, M-ID of -1665883002 *Jun 3 06:02:46.526: ISAKMP:(2008):QM Initiator gets spi *Jun 3 06:02:46.530: ISAKMP:(2008): sending packet to 172.16.186.186 my_port 500 peer_port 500 (I) QM_IDLE *Jun 3
06:02:46.530: ISAKMP:(2008):Node -1665883002, Input = IKE_MSG_INTERNAL, IKE_INIT_QM *Jun 3
06:02:46.530: ISAKMP:(2008):Old State = IKE_QM_READY New State = IKE_QM_I_QM1 *Jun 3
06:02:46.538: ISAKMP (0:2008): received packet from 172.16.186.186 dport 500 sport 500 Global (I) QM_IDLE *Jun 3 06:02:46.538: ISAKMP:(2008): processing HASH payload. message ID = -1665883002 *Jun 3 06:02:46.538: ISAKMP:(2008): processing SA payload. message ID = -1665883002 *Jun 3 06:02:46.538: ISAKMP:(2008):Checking IPsec proposal 1 *Jun 3 06:02:46.538: ISAKMP: transform 1, ESP_3DES *Jun 3 06:02:46.538: ISAKMP: attributes in transform: *Jun 3 06:02:46.538: ISAKMP: encaps is 1 (Tunnel) *Jun 3 06:02:46.538: ISAKMP: SA life type in seconds *Jun 3
06:02:46.538: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B *Jun 3 06:02:46.538: ISAKMP: SA life type in kilobytes *Jun 3 06:02:46.538: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 *Jun 3 06:02:46.542: ISAKMP: authenticator is HMAC-SHA *Jun 3 06:02:46.542: ISAKMP:(2008):atts are acceptable. *Jun 3 06:02:46.542: IPSEC(validate_proposal_request): proposal part #1 *Jun 3 06:02:46.542: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 172.16.186.130, remote= 172.16.186.186, local_proxy= 10.12.130.1/255.255.255.255/0/0 (type=1), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-sha-hmac (Tunnel), lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0 *Jun 3 06:02:46.542: Crypto mapdb : proxy_match src addr : 10.12.130.1 dst addr : 0.0.0.0 protocol : 0 src port : 0 dst port : 0 *Jun 3 06:02:46.542: ISAKMP:(2008): processing NONCE payload. message ID = -1665883002 *Jun 3 06:02:46.542: ISAKMP:(2008): processing ID payload. message ID = -1665883002 *Jun 3 06:02:46.542: ISAKMP:(2008): processing NOTIFY RESPONDER_LIFETIME protocol 3 spi 1752561220, message ID = -1665883002, sa = 83BCC9DC *Jun 3
06:02:46.542: ISAKMP:(2008):SA authentication status: authenticated *Jun 3 06:02:46.542: ISAKMP:(2008): processing responder lifetime *Jun 3 06:02:46.542: ISAKMP (2008): responder lifetime of 3600s *Jun 3 06:02:46.542: ISAKMP:(2008): Creating IPsec SAs *Jun 3 06:02:46.542: inbound SA from 172.16.186.186 to 172.16.186.130 (f/i) 0/ 0 (proxy 0.0.0.0 to 10.12.130.1) *Jun 3 06:02:46.542: has spi 0x29354010 and conn_id 0 *Jun 3 06:02:46.542: lifetime of 3590 seconds *Jun 3 06:02:46.542: lifetime of 4608000 kilobytes *Jun 3 06:02:46.546: outbound SA from 172.16.186.130 to 172.16.186.186 (f/i) 0/0 (proxy 10.12.130.1 to 0.0.0.0) *Jun 3 06:02:46.546: has spi 0x6875F644 and conn_id 0 *Jun 3 06:02:46.546: lifetime of 3590 seconds *Jun 3
06:02:46.546: lifetime of 4608000 kilobytes *Jun 3 06:02:46.546: ISAKMP:(2008): sending packet to 172.16.186.186 my_port 500 peer_port 500 (I) QM_IDLE *Jun 3 06:02:46.546: ISAKMP:(2008):deleting node -1665883002 error FALSE reason "No Error" *Jun 3 06:02:46.546: ISAKMP:(2008):Node -1665883002, Input = IKE_MSG_FROM_PEER, IKE_QM_EXCH *Jun 3 06:02:46.546: ISAKMP:(2008):Old State = IKE_QM_I_QM1 New State = IKE_QM_PHASE2_COMPLETE *Jun 3 06:02:46.546: IPSEC(key_engine): got a queue event with 1 KMI message(s) *Jun 3 06:02:46.546: Crypto mapdb : proxy_match src addr : 10.12.130.1 dst addr : 0.0.0.0 protocol : 0 src port : 0 dst port : 0 *Jun 3 06:02:46.546: IPSEC(crypto_ipsec_sa_find_ident_head): reconnecting with the same proxies and peer 172.16.186.186 *Jun 3 06:02:46.546: IPSEC(policy_db_add_ident): src 10.12.130.1, dest 0.0.0.0, dest_port 0 *Jun 3 06:02:46.546: IPSEC(create_sa): sa created, (sa) sa_dest= 172.16.186.130, sa_proto= 50, sa_spi= 0x29354010(691355664), sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 11 *Jun 3 06:02:46.546: IPSEC(create_sa): sa created, (sa) sa_dest= 172.16.186.186, sa_proto= 50, sa_spi= 0x6875F644(1752561220), sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 12 *Jun 3 06:02:46.550: IPSEC(update_current_outbound_sa): updated peer 172.16.186.186 current outbound sa to SPI 6875F644 *Jun 3 06:02:46.550: %CRYPTO-6-EZVPN_CONNECTION_UP: (Client) User= Group=vpngrp Client_public_addr=172.16.186.130 Server_public_addr=172.16.186.186 NEM_Remote_Subnets=10.12.130.1/255.255.255.255 *Jun 3 06:02:47.130: ISAKMP: set new node -1866551769 to QM_IDLE

関連情報

- [Cisco Easy VPN 製品のサポート](#)
- [IOS ルータ：分割トンネリング 設定例のネットワーク拡張モード（NEM）の Easy VPN（EzVPN）](#)
- [Cisco VPN クライアント](#)
- [IPSec ネゴシエーション/IKE プロトコル](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)