

RADIUS をユーザ認証に使用する Cisco IOS ルータと Cisco VPN Client 4.x for Windows の間の IPSec 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](#)

[2621XM ルータの設定](#)

[RADIUS サーバの設定](#)

[ユーザ認証のための RADIUS サーバの設定](#)

[VPN Client 4.8 の設定](#)

[スプリットトンネリングの有効化](#)

[設定 RADIUSサーバ フォールバック 機能](#)

[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](#)

[デバッグ出力](#)

[関連情報](#)

概要

このドキュメントでは、Remote Authentication Dial-In User Service (RADIUS) をユーザ認証に使用するルータと Cisco VPN Client 4.x の間の接続を設定する方法について説明しています。Cisco IOS® ソフトウェアリリース 12.2(8)T およびそれ以降は Cisco VPN Client 4.x からの接続をサポートします。VPN Clients 3.x と 4.x では Diffie Hellman (DH) グループ 2 ポリシーを使用しています。isakmp policy # group 2 コマンドを使用すると VPN Client の接続が有効になります。

この資料は RADIUSサーバの認証、および許可を示したものです (Windows Internet Naming Service (WINS) および Domain Naming Service (DNS を割り当てることのような)) ローカルでルータによって。RADIUS サーバを認証と認可の両方に使用する場合は、『[Cisco IOS ルータと Cisco VPN Client 4.x for Windows 間の RADIUS を使用した IPSec の設定](#)』を参照してください。

注: IPSec VPN アカウティングは現在使用可能です。詳細と設定例は、『[IPSec VPN アカウティング](#)』を参照してください。

TACACS+ プロトコルを使用して外部でユーザ認証を行うシナリオについての詳細は、『[TACACS+ ユーザ認証を使用する IOS ルータと Cisco VPN Client 4.x for Windows の間の IPsec トンネルの設定例](#)』を参照してください。

Cisco IOS ルータでローカルにユーザ認証を行うシナリオについての詳細は、『[ローカル拡張認証を使用する IOS に対する Cisco VPN Client 3.x for Windows の設定](#)』を参照してください。

Microsoft Windows 2003 Internet Authentication Service (IAS) RADIUS サーバを使用して Cisco VPN Client (4.x for Windows) と PIX 500 シリーズ セキュリティ アプライアンス 7.x の間にリモート アクセス VPN 接続を設定する方法については、『[Windows 2003 IAS RADIUS サーバの Active Directory 認証を使用した PIX/ASA 7.x と Cisco VPN Client 4.x 間のリモートアクセス VPN の設定例](#)』を参照してください。

ワイルドカード、モード設定、`sysopt connection permit-ipsec` コマンド、拡張認証 (Xauth) を使用して VPN Client を PIX Firewall に接続する方法については、『[拡張認証による IPsec - PIX から Cisco Secure VPN クライアントへのワイルドカード、事前共有、モード設定](#)』を参照してください。

RADIUS をユーザ認証とアカウントिंगに使用して Cisco VPN 3000 コンセントレータと Cisco VPN Client 4.x for Windows の間に IPsec トンネルを確立する方法については、『[RADIUS を使用した VPN 3000 コンセントレータと VPN Client 4.x for Windows 間のユーザ認証とアカウントिंगのための IP セキュリティ設定例](#)』を参照してください。

[前提条件](#)

[要件](#)

この設定を行う前に、次の要件が満たされていることを確認します。

- IPsec 用に割り当てるためのアドレスのプール
- パスワードが「cisco123」に設定された「3000clients」という名前のグループ
- RADIUS サーバでのユーザ認証

[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 ソフトウェア リリース 12.2(15)T2 が稼働する 2621XM ルータ
- Windows 2000 バージョンのための CiscoSecure ACS 4.2 (どの RADIUSサーバでもはたらく必要があります)
- Cisco VPN Client for Windows バージョン 4.8 (任意の VPN Client 4.x 以降で使用可能)

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。

次の出力は、ルータで `show version` コマンドを発行した結果です。

```
vpn2621#show version Cisco Internetwork Operating System Software IOS (tm) C2600 Software (C2600-IK9S-M), Version 12.2(15)T2, RELEASE SOFTWARE (fc2) TAC Support: http://www.cisco.com/tac Copyright (c) 1986-2003 by cisco Systems, Inc. Compiled Thu 01-May-03 10:39 by nmasa Image text-
```

base: 0x80008098, data-base: 0x81BBB0BC ROM: System Bootstrap, Version 12.2(7r) [cmong 7r],
RELEASE SOFTWARE (fcl) vpn2621 uptime is 1 hour, 34 minutes System returned to ROM by reload
System image file is "flash:c2600-ik9s-mz.122-15.T2.bin" This product contains cryptographic
features and is subject to United States and local country laws governing import, export,
transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority
to import, export, distribute or use encryption. Importers, exporters, distributors and users
are responsible for compliance with U.S. and local country laws. By using this product you agree
to comply with applicable laws and regulations. If you are unable to comply with U.S. and local
laws, return this product immediately. A summary of U.S. laws governing Cisco cryptographic
products may be found at: <http://www.cisco.com/wwl/export/crypto/tool/stqrg.html> If you require
further assistance please contact us by sending email to export@cisco.com. cisco 2621XM
(MPC860P) processor (revision 0x100) with 125952K/5120K bytes of memory. Processor board ID
JAD064503FK (64188517) M860 processor: part number 5, mask 2 Bridging software. X.25 software,
Version 3.0.0. 2 FastEthernet/IEEE 802.3 interface(s) 2 Serial(sync/async) network interface(s)
1 terminal line(s) 1 Virtual Private Network (VPN) Module(s) 1 cisco content engine(s) 32K bytes
of non-volatile configuration memory. 32768K bytes of processor board System flash (Read/Write)
Configuration register is 0x2102

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。

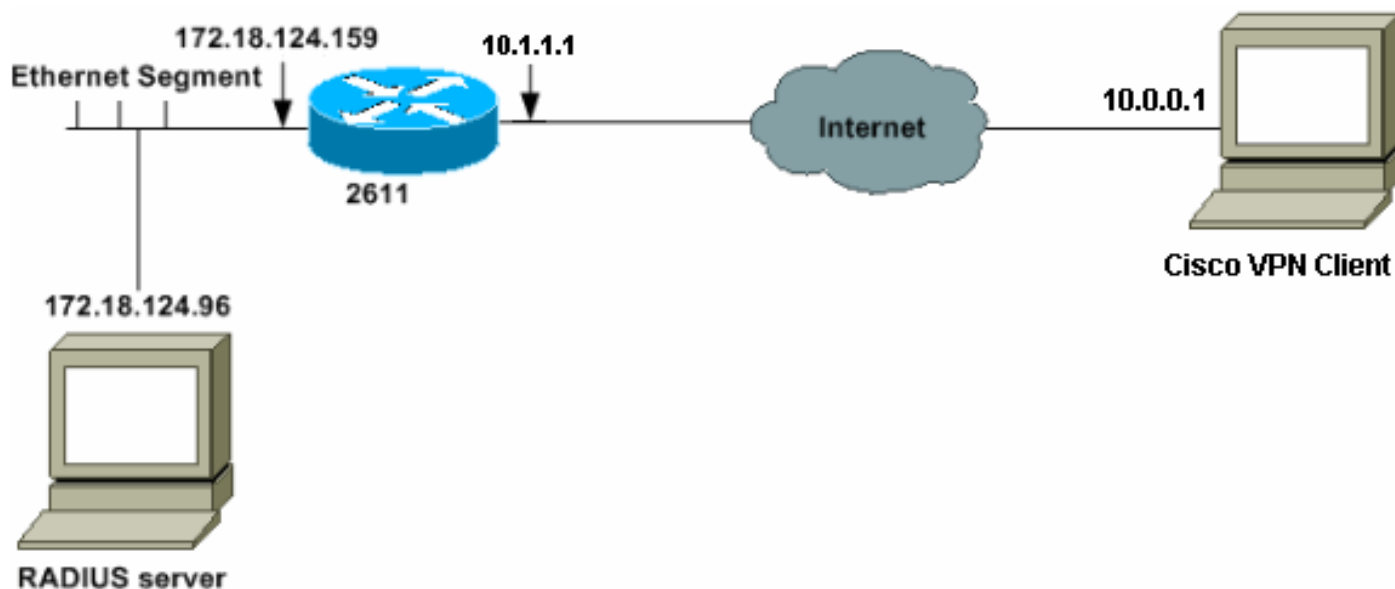
設定

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。



2621XM ルータの設定

2621XM ルータ

```
!--- Enable authentication, authorization and accounting
(AAA) !--- for user authentication and group
authorization. aaa new-model ! !--- In order to enable
extended authentication (Xauth) for user authentication,
!--- enable the aaa authentication commands. !--- "Group
radius local" specifies RADIUS user authentication !---
to be used by default and to use local database if
RADIUS server is not reachable. aaa authentication login
userauthen group radius local !--- In order to enable
group authorization, !--- enable the aaa authorization
commands. aaa authorization network groupauthor local !-
-- 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
that will be used to specify the !--- Windows Internet
Naming Service (WINS) and Domain Naming Service (DNS)
server !--- addresses to the client, along with the pre-
shared key for authentication. crypto isakmp client
configuration group 3000client key cisco123 dns
10.1.1.10 wins 10.1.1.20 domain cisco.com pool ippool !
!--- 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. crypto dynamic-map
dynmap 10 set transform-set myset ! !--- Create the
actual crypto map, !--- and apply the AAA lists that
were created earlier. crypto map clientmap client
authentication list userauthen crypto map clientmap
isakmp authorization list groupauthor crypto map
clientmap client configuration address respond crypto
map clientmap 10 ipsec-isakmp dynamic dynmap !--- Apply
the crypto map on the outside interface. interface
Ethernet0/0 ip address 10.1.1.1 255.255.255.0 half-
duplex crypto map clientmap interface Ethernet0/1 ip
address 172.18.124.159 255.255.255.0 half-duplex ! !---
Create a pool of addresses to be assigned to the VPN
Clients. ip local pool ippool 10.16.20.1 10.16.20.200 ip
classless ip route 0.0.0.0 0.0.0.0 10.1.1.2 ip http
server ip pim bidir-enable ! ! ! !--- Specify the IP
address of the RADIUS server, !--- along with the RADIUS
shared secret key. radius-server host 172.18.124.96
auth-port 1645 acct-port 1646 key cisco123 radius-server
retransmit 3
```

RADIUS サーバの設定

ユーザ認証のための RADIUS サーバの設定

RADIUS サーバを設定するには、次の手順を実行します。

1. RADIUS サーバ データベースで、ルータのエントリを追加します。

AAA Client Hostname	AAA Client IP Address	Authenticate Using
340	172.18.124.151	RADIUS (Cisco Aironet)
Aironet-340-Lab	14.36.1.99	RADIUS (Cisco Aironet)
glenntest	172.18.124.120	RADIUS (Cisco IOS/PIX)
router	172.18.124.150	TACACS+ (Cisco IOS)

[Add Entry](#)

- [Network Device Groups](#)
- [Adding a Network Device Group](#)
- [Renaming a Network Device Group](#)
- [Deleting a Network Device Group](#)
- [AAA Clients](#)
- [Adding a AAA Client](#)
- [Editing a AAA Client](#)
- [Deleting a AAA Client](#)
- [AAA Servers](#)
- [Adding a AAA Server](#)
- [Editing a AAA Server](#)
- [Deleting a AAA Server](#)
- [Proxy Distribution Table](#)
- [Adding a Proxy Distribution Table Entry](#)
- [Sorting Proxy Distribution Table Entries](#)

2. 共有秘密鍵「cisco123」とともに、ルータの IP アドレス「172.18.124.159」を指定します。Authenticate Using ドロップダウン ボックスで RADIUS を選択します。

Add AAA Client

AAA Client Hostname:

AAA Client IP Address:

Key:

Authenticate Using:

Single Connect TACACS+ AAA Client (Record stop in accounting on failure).

Log Update/Watchdog Packets from this AAA Client

Log RADIUS Tunneling Packets from this AAA Client

[Submit](#) [Submit + Restart](#) [Cancel](#)

- [AAA Client Hostname](#)
- [AAA Client IP Address](#)
- [Key](#)
- [Network Device Group](#)
- [Authenticate Using](#)
- [Single Connect TACACS+ AAA Client](#)
- [Log Update/Watchdog Packets from this AAA Client](#)
- [Log RADIUS Tunneling Packets from this AAA Client](#)

AAA Client Hostname

The AAA Client Hostname is the name assigned to the AAA client.

[\[Back to Top\]](#)

AAA Client IP Address

3. CiscoSecure データベースで、VPN ユーザのユーザ名を追加します。この例では、ユーザ名は cisco です。

User: [Find](#) [Add/Edit](#)

List users beginning with letter/number:

A B C D E F G H I J K L M
 N O P Q R S T U V W X Y Z
 0 1 2 3 4 5 6 7 8 9

[List All Users](#)

[Back to Help](#)

- [User Setup and External User Databases](#)
- [Finding a Specific User in the CiscoSecure User Database](#)
- [Adding a User to the CiscoSecure User Database](#)
- [Listing Usernames that Begin with a Particular Character](#)
- [Listing All Usernames in the CiscoSecure User Database](#)
- [Changing a Username in the CiscoSecure User Database](#)

User Setup enables you to configure individual user information, add users, and delete users in the database.

4. 次のウィンドウで、ユーザ cisco のパスワードを指定します。この例では、パスワードも cisco です。ユーザ アカウントをグループにマッピングできます。完了したら、Submit をクリックします。

Supplementary User Info

Real Name
Description

User Setup

Password Authentication:
CiscoSecure Database

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password
Confirm Password

Separate (CHAP/MS-CHAP/ARAP)
Password
Confirm Password

When using a Token Card server for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Group to which the user is assigned:
Group 19

Submit Cancel

- [Account Disabled](#)
- [Deleting a Username](#)
- [Supplementary User Info](#)
- [Password Authentication](#)
- [Group to which the user is assigned](#)
- [Callback](#)
- [Client IP Address Assignment](#)
- [Advanced Settings](#)
- [Network Access Restrictions](#)
- [Max Sessions](#)
- [Usage Quotas](#)
- [Account Disable](#)
- [Downloadable ACLs](#)
- [Advanced TACACS+ Settings](#)
- [TACACS+ Enable Control](#)
- [TACACS+ Enable Password](#)
- [TACACS+ Outbound Password](#)
- [TACACS+ Shell Command Authorization](#)
- [TACACS+ Unknown Services](#)
- [IETF RADIUS Attributes](#)
- [RADIUS Vendor-Specific Attributes](#)

Account Disabled Status

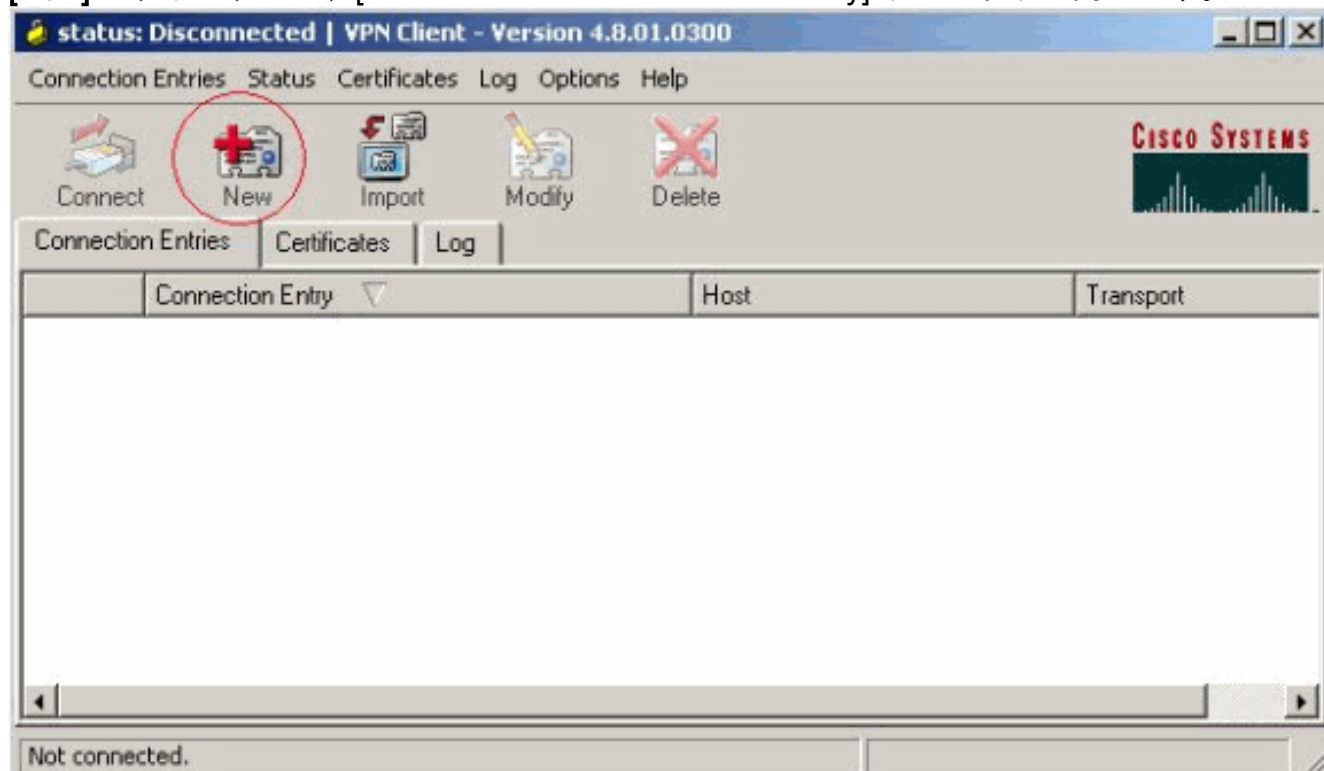
Select the Account Disabled check box to disable this account; clear the check box to enable the account.

[\[Back to Top\]](#)

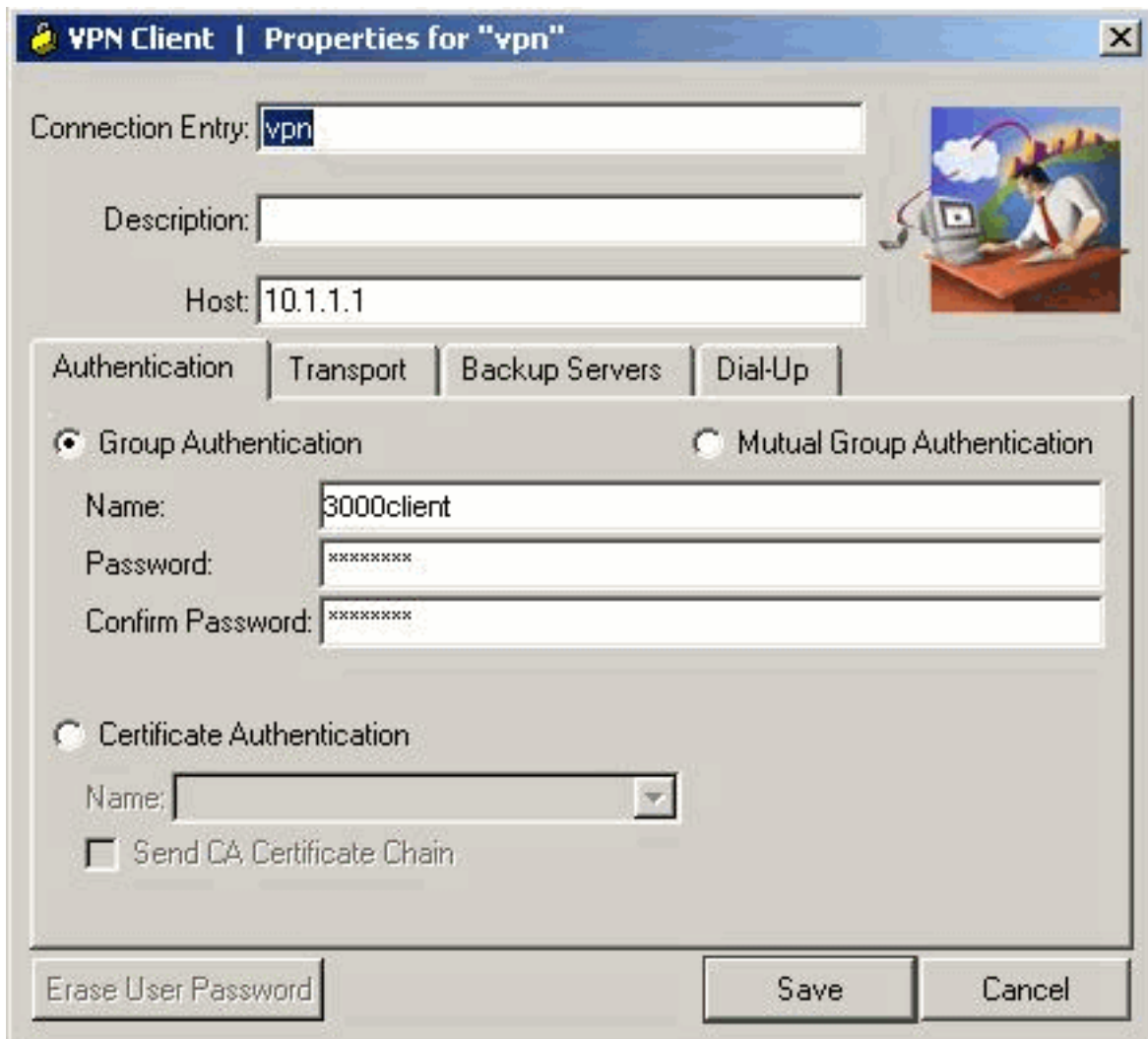
[VPN Client 4.8 の設定](#)

VPN Client 4.8 を設定するには、次の手順を実行します。

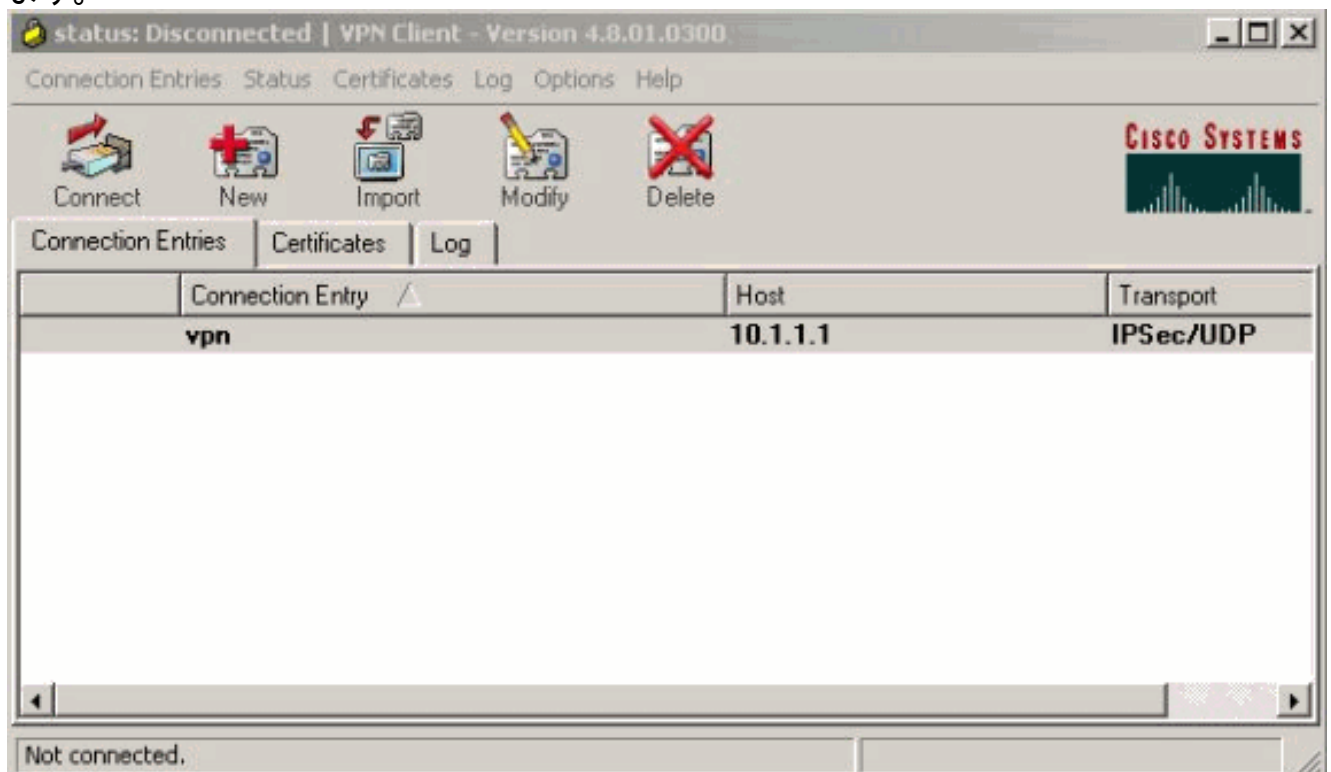
1. [Start] > [Programs] > [Cisco Systems VPN Client] > [VPN Client] の順に選択します。
2. **[New]** をクリックして、[Create New VPN Connection Entry] ウィンドウを開きます。



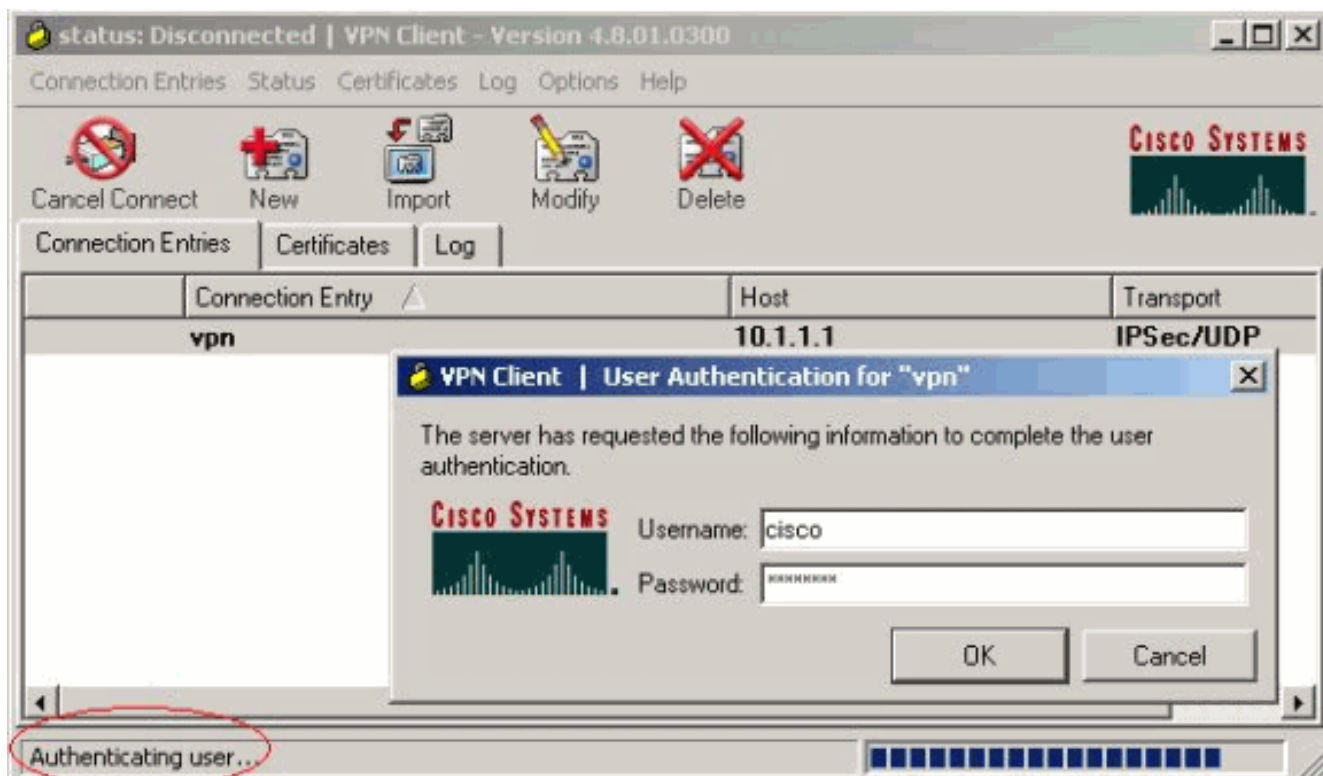
3. 接続エントリの名前と説明を入力します。Host ボックスに、ルータの Outside の IP アドレスを入力します。次に、VPN グループ名とパスワードを入力し、**[Save]** をクリックします。



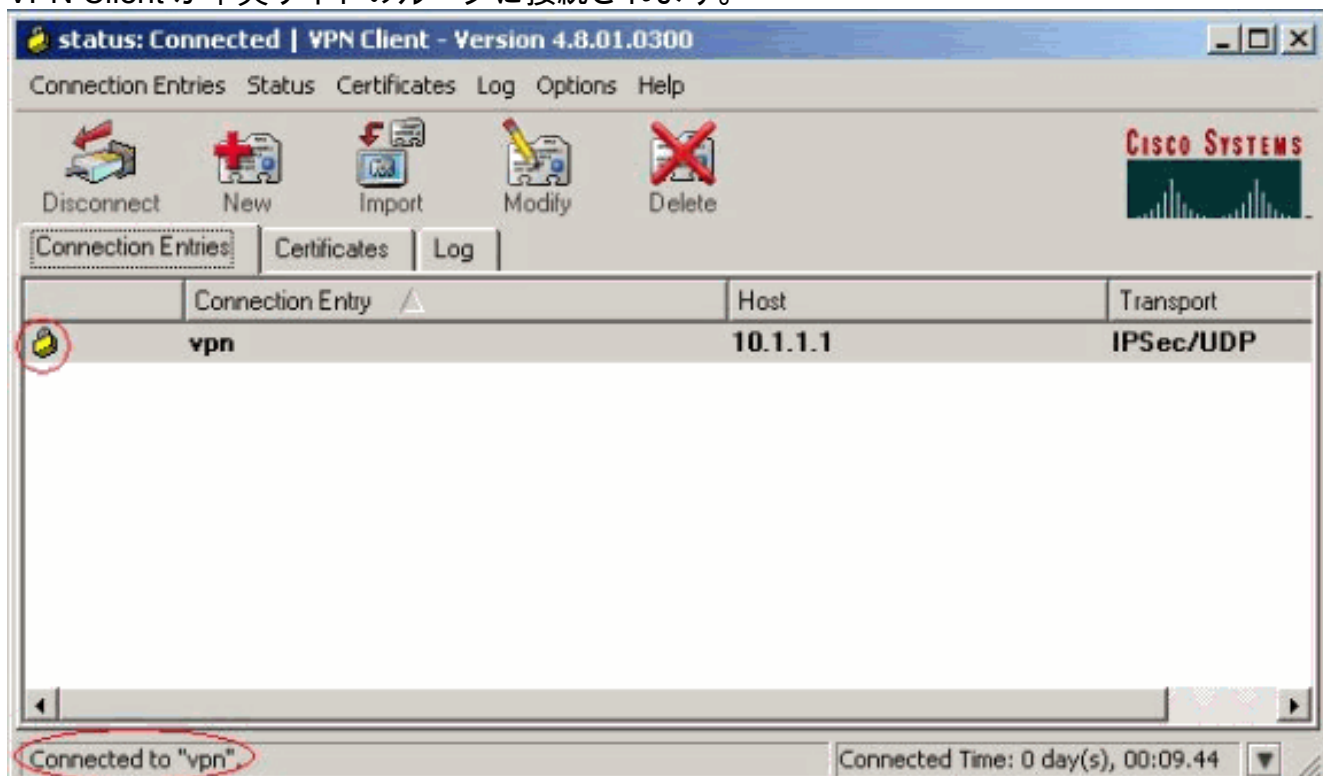
4. 使用する接続をクリックし、VPN Client のメイン ウィンドウから [Connect] をクリックします。



5. ダイアログボックスが表示されたら、Xauth のユーザ名とパスワード情報を入力して [OK] をクリックし、リモート ネットワークに接続します。



VPN Client が中央サイトのルータに接続されます。



スプリット トンネリングの有効化

VPN 接続のスプリット トンネリングを有効にするには、ルータでアクセス コントロール リスト (ACL) を設定してあることを確認してください。この例では、`access-list 108` コマンドがスプリット トンネリング用のグループに関連付けられており、トンネルは `172.18.124.X/24` ネットワークに対して形成されます。トラフィックは暗号化されず ACL 108 以外のデバイス (インターネットなど) に送信されます。

```
access-list 108 permit ip 172.18.124.0 0.0.255.255 10.16.20.0 0.0.0.255
```


グループプロパティで ACL を適用します。

```
crypto isakmp client configuration group 3000client
key cisco123
dns 10.1.1.10 wins 10.1.1.20 domain cisco.com pool ippool acl 108
```

[RADIUSサーバフォールバック機能を設定して下さい](#)

プライマリ RADIUS サーバが使用不能になると、ルータは次にアクティブなバックアップ RADIUS サーバにフェールオーバーします。ルータはプライマリサーバが利用できてセカンダリ RADIUS サーバを永久に使用し続けます。通常、プライマリサーバはパフォーマンスが高く、優先サーバとなっています。セカンダリサーバが利用できない場合、ローカルデータベースは [AAA認証ログイン](#) を使用して認証に [userauthen group radius ローカルコマンド](#) を使用することができます。

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。

次に、関連する **show** コマンドの出力を示します。

```
vpn2621#show crypto isakmp sa dst src state conn-id slot 10.1.1.1 10.0.0.1 QM_IDLE 3 0
vpn2621#show crypto ipsec sa interface: Ethernet0/0 Crypto map tag: clientmap, local addr.
10.1.1.1 local ident (addr/mask/prot/port): (10.1.1.1/255.255.255.255/0/0) remote ident
(addr/mask/prot/port): (10.16.20.2/255.255.255.255/0/0) current_peer: 10.0.0.1 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 decompress failed: 0 #send errors 0, #recv errors 0 local crypto endpt.:
10.1.1.1, remote crypto endpt.: 10.0.0.1 path mtu 1500, media mtu 1500 current outbound spi:
77AFCCFA inbound esp sas: spi: 0xC7AC22AB(3349947051) transform: esp-3des esp-sha-hmac , in use
settings = {Tunnel, } slot: 0, conn id: 2000, flow_id: 1, crypto map: clientmap sa timing:
remaining key lifetime (k/sec): (4608000/3444) IV size: 8 bytes replay detection support: Y
inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0x77AFCCFA(2008009978) transform: esp-
3des esp-sha-hmac , in use settings = {Tunnel, } slot: 0, conn id: 2001, flow_id: 2, crypto map:
clientmap sa timing: remaining key lifetime (k/sec): (4608000/3444) IV size: 8 bytes replay
detection support: Y outbound ah sas: outbound pcp sas: local ident (addr/mask/prot/port):
(172.18.124.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port):
(10.16.20.2/255.255.255.255/0/0) current_peer: 10.0.0.1 PERMIT, flags={} #pkts encaps: 4, #pkts
encrypt: 4, #pkts digest 4 #pkts decaps: 6, #pkts decrypt: 6, #pkts verify 6 #pkts compressed:
0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress
failed: 0 #send errors 0, #recv errors 0 local crypto endpt.: 10.1.1.1, remote crypto endpt.:
10.0.0.1 path mtu 1500, media mtu 1500 current outbound spi: 2EE5BF09 inbound esp sas: spi:
0x3565451F(895829279) transform: esp-3des esp-sha-hmac , in use settings = {Tunnel, } slot: 0,
conn id: 2002, flow_id: 3, crypto map: clientmap sa timing: remaining key lifetime (k/sec):
(4607999/3469) IV size: 8 bytes replay detection support: Y inbound ah sas: inbound pcp sas:
outbound esp sas: spi: 0x2EE5BF09(786808585) transform: esp-3des esp-sha-hmac , in use settings
= {Tunnel, } slot: 0, conn id: 2003, flow_id: 4, crypto map: clientmap sa timing: remaining key
lifetime (k/sec): (4607999/3469) IV size: 8 bytes replay detection support: Y outbound ah sas:
outbound pcp sas:
vpn2621#show crypto engine connections active
ID Interface IP-Address State
Algorithm Encrypt Decrypt 3 Ethernet0/0 10.1.1.1 set HMAC_SHA+3DES_56_C 0 0 2000 Ethernet0/0
10.1.1.1 set HMAC_SHA+3DES_56_C 0 5 2001 Ethernet0/0 10.1.1.1 set HMAC_SHA+3DES_56_C 5 0 2002
Ethernet0/0 10.1.1.1 set HMAC_SHA+3DES_56_C 0 6 2003 Ethernet0/0 10.1.1.1 set HMAC_SHA+3DES_56_C
4 0
vpn2621#show crypto engine accelerator statistic
Virtual Private Network (VPN) Module in aim
slot : 0
Statistics for Hardware VPN Module since the last clear of counters 5570 seconds ago
14 packets in 14 packets out 0 packet overruns 0 output packets dropped 0 packets decompressed 0
```

packets compressed 0 compressed bytes in 0 uncompressed bytes in 0 decompressed bytes out 0 compressed bytes out 0 packets bypass compression 0 packets abort compression 0 packets fail decompression 0 packets fail compression 7 packets decrypted 7 packets encrypted 532 bytes decrypted 532 bytes encrypted 784 bytes before decrypt 19200 bytes after encrypt 0 paks/sec in 0 paks/sec out 0 Kbits/sec decrypted 0 Kbits/sec encrypted Last 5 minutes: 14 packets in 14 packets out 7 packets decrypted 7 packets encrypted 532 bytes decrypted 420 bytes encrypted 784 bytes before decrypt 672 bytes after encrypt 0 paks/sec in 0 paks/sec out 0 Kbits/sec decrypted 0 Kbits/sec encrypted rx_no_endp: 0 rx_hi_discards: 0 fw_failure: 0 invalid_sa: 0 invalid_flow: 0 cgx_errors 0 fw_qs_filled: 0 fw_resource_lock: 0 lotx_full_err: 0 null_ip_error: 0 pad_size_error: 0 out_bound_dh_acc: 0 esp_auth_fail: 0 ah_auth_failure: 0 crypto_pad_error: 0 ah_prot_absent: 0 ah_seq_failure: 0 ah_spi_failure: 0 esp_prot_absent: 0 esp_seq_fail: 0 esp_spi_failure: 0 obound_sa_acc: 0 invalid_sa: 0 out_bound_sa_flow: 0 invalid_dh: 0 bad_keygroup: 0 out_of_memory: 0 no_sh_secret: 0 no_skeys: 0 invalid_cmd: 0 dsp_coproc_err: 0 comp_unsupported: 0 pak_too_big: 0 null packets: 0 pak_mp_length_spec_fault: 0 cmd queue errors: 0 tx_lo_queue_size_max 0 cmd_unimplemented: 0 Interrupts: 439 Immed: 0 HiPri ints: 14 LoPri ints: 425 POST Errs: 0 Alerts: 0 Unk Cmds: 0 UnexpCmds: 0 cgx_cmd_pending:0 packet_loop_max: 0packet_loop_limit: 0 vpn2621#sh crypto engine configuration crypto engine name: Virtual Private Network (VPN) Module crypto engine type: hardware Product Name: AIM-VPN/BP Configuration: 0x000109010F00F00784000000 : 0x995FB1441BA279D5BD46CF6C : 0xECE77614C30835CB0A000300 : 0x00000000000000000000000000000000 CryptIC Version: 001.000 CGX Version: 001.009 CGX Reserved: 0x000F PCDB info: 0x07F0 0x0084 0x0000 Serial Number: 0x5F9944B1A21BD57946BD : 0x6CCFE7EC14768C3CB35 DSP firmware version: 000.010 DSP Bootstrap Version: 000.003 DSP Bootstrap Info: 0x0000 Compression: Yes DES: Yes 3 DES: Yes AES CBC: No AES CNTR: No Maximum buffer length: 4096 Maximum DH index: 0210 Maximum SA index: 0420 Maximum Flow index: 0840 Maximum RSA key size: 0000 crypto engine in slot: 0 platform: VPN hardware accelerator Crypto Adjacency Counts: Lock Count: 0 Unlock Count: 0 crypto lib version: 16.0.0 ipsec lib version: 2.0.0

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

[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。

- **debug crypto ipsec** : IPsec 接続に関するデバッグ情報を表示します。
- **debug crypto isakmp** : IPSec 接続に関するデバッグ情報を表示し、両端で互換性がないために拒否された最初の属性セットを表示します。
- **debug crypto engine** : 暗号化エンジンからの情報を表示します。
- **debug aaa authentication** : AAA/Terminal Access Controller Access Control System Plus (TACACS+) 認証に関する情報を表示します。
- **debug aaa authorization radius** : AAA/TACACS+ 認証に関する情報を表示します。
- **debug radius** : RADIUS サーバとルータの間のトラブルシューティング通信に関する情報を表示します。

デバッグ出力

このセクションでは、設定のトラブルシューティングに役立つルータのデバッグ情報を説明しています。

ルータのログ

vpn2621#show debug General OS: AAA Authentication debugging is on AAA Authorization debugging is on Radius protocol debugging is on Radius packet protocol debugging is on Cryptographic Subsystem: Crypto ISAKMP debugging is on Crypto Engine debugging is on Crypto IPSEC debugging is on vpn2621# *ISAKMP (0:0): **received packet from 10.0.0.1 dport 500 sport 500 Global (N) NEW SA** *ISAKMP: Created a peer struct for 10.0.0.1, peer port 500 *ISAKMP: Locking peer struct 0x83166B20, IKE refcount 1 for crypto_ikmp_config_initialize_sa *ISAKMP (0:0): Setting client config settings 82F0F82C *ISAKMP (0:0): (Re)Setting client xauth list and state *ISAKMP: local port 500, remote port 500 *ISAKMP: insert sa successfully sa = 83165694 *ISAKMP (0:1): processing SA payload. message ID = 0 *ISAKMP (0:1): processing ID payload. message ID = 0 *ISAKMP (0:1): peer matches *none* of the profiles *ISAKMP (0:1): processing vendor id payload *ISAKMP (0:1): vendor ID seems Unity/DPD but major 215 mismatch *ISAKMP (0:1): vendor ID is XAUTH *ISAKMP (0:1): processing vendor id payload *ISAKMP (0:1): vendor ID is DPD *ISAKMP (0:1): processing vendor id payload *ISAKMP (0:1): vendor ID seems Unity/DPD but major 123 mismatch *ISAKMP (0:1): vendor ID is NAT-T v2 *ISAKMP (0:1): processing vendor id payload *ISAKMP (0:1): vendor ID seems Unity/DPD but major 194 mismatch *ISAKMP (0:1): processing vendor id payload *ISAKMP (0:1): vendor ID is Unity *ISAKMP (0:1) Authentication by xauth preshared *ISAKMP (0:1): Checking ISAKMP transform 1 against priority 3 policy *ISAKMP: encryption AES-CBC *ISAKMP: hash SHA *ISAKMP: default group 2 *ISAKMP: auth XAUTHInitPreShared *ISAKMP: life type in seconds *ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B *ISAKMP: keylength of 256 *ISAKMP (0:1): Encryption algorithm offered does not match policy!
/en/US/docs/net_mgmt/wan_service_administrator/1.1/administrator/guide/getstart.html -
snip/en/US/docs/net_mgmt/wan_service_administrator/1.1/administrator/guide/getstart.html
/en/US/docs/net_mgmt/wan_service_administrator/1.1/administrator/guide/getstart.html
/en/US/docs/net_mgmt/wan_service_administrator/1.1/administrator/guide/getstart.html *!--- ISAKMP values are acceptable and then the router continues with the !--- ISAKMP negotiation process.*
***ISAKMP (0:1): Checking ISAKMP transform 9 against priority 3 policy *ISAKMP: encryption 3DES-CBC *ISAKMP: hash SHA *ISAKMP: default group 2 *ISAKMP: auth XAUTHInitPreShared *ISAKMP: life type in seconds *ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B *ISAKMP (0:1): atts are acceptable. Next payload is 3** *CryptoEngine0: generate alg parameter *CryptoEngine0: CRYPTO_ISA_DH_CREATE(hw)(ipsec) *CRYPTO_ENGINE: Dh phase 1 status: 0 *ISAKMP (0:1): processing KE payload. message ID = 0 *CryptoEngine0: generate alg parameter *CryptoEngine0: CRYPTO_ISA_DH_SHARE_SECRET(hw)(ipsec) *ISAKMP (0:1): processing NONCE payload. message ID = 0 *ISAKMP (0:1): vendor ID is NAT-T v2 *AAA: parse name=ISAKMP-ID-AUTH idb type=-1 tty=-1 *AAA/MEMORY: create_user (0x830E12E8) user='3000client' ruser='NULL' ds0=0 port='ISAKMP-ID-AUTH' rem_addr='10.0.0.1' authen_type=NONE service=LOGIN priv=0 initial_task_id='0', vrf= (id=0) *ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH *ISAKMP (0:1): Old State = IKE_READY New State = IKE_R_AM_AAA_AWAIT *ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(54534875): Port='ISAKMP-ID-AUTH' list='groupauthor' service=NET *AAA/AUTHOR/CRYPTO AAA: ISAKMP-ID-AUTH(54534875) user='3000client' *ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(54534875): send AV service=ike *ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(54534875): send AV protocol=ipsec *ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(54534875): found list "groupauthor" *ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(54534875): Method=LOCAL *AAA/AUTHOR (54534875): Post authorization status = PASS_ADD *ISAKMP: got callback 1 * AAA/AUTHOR/IKE: Processing AV service=ike * AAA/AUTHOR/IKE: Processing AV protocol=ipsec * AAA/AUTHOR/IKE: Processing AV tunnel-password=cisco123 * AAA/AUTHOR/IKE: Processing AV default-domain*cisco.com * AAA/AUTHOR/IKE: Processing AV addr-pool*ippool * AAA/AUTHOR/IKE: Processing AV key-exchange=ike * AAA/AUTHOR/IKE: Processing AV group-lock*0 * AAA/AUTHOR/IKE: Processing AV timeout*0 * AAA/AUTHOR/IKE: Processing AV idletime*0 * AAA/AUTHOR/IKE: Processing AV inacl*108 * AAA/AUTHOR/IKE: Processing AV dns-servers*10.1.1.10 0.0.0.0 * AAA/AUTHOR/IKE: Processing AV wins-servers*10.1.1.20 0.0.0.0 *CryptoEngine0: create ISAKMP SKEYID for conn id 1 *CryptoEngine0: CRYPTO_ISA_SA_CREATE(hw)(ipsec) *ISAKMP (0:1): SKEYID state generated *ISAKMP (0:1): constructed NAT-T vendor-02 ID *ISAKMP (0:1): SA is doing pre-shared key authentication plus XAUTH using id type ID_IPV4_ADDR *ISAKMP (1): ID payload next-payload : 10 type : 1 addr : 10.1.1.1 protocol : 17 port : 0 length : 8 *ISAKMP (1): Toine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec) *ISAKMP (0:1): processing HASH payload. message ID = 0 *CryptoEngine0: generate hmac context for conn id 1 *CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)tal payload length: 12 *CryptoEngine0: generate hmac conte *ISAKMP (0:1): processing NOTIFY INITIAL_CONTACT protocol 1 spi 0, message ID = 0, sa = 83165694 *ISAKMP (0:1): Process initial contact, bring down existing phase 1 and 2 SA's with local 10.1.1.1 remote 10.0.0.1 remote port 500 *ISAKMP (0:1): returning IP addr to the address pool *ISAKMP:received payload type 17 *ISAKMP (0:1): Detected NAT-D payload *ISAKMP (0:1): recalc my hash for NAT-D *ISAKMP (0:1): NAT match MINE hash *ISAKMP:received payload type 17xt for conn id 1 *CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec) *ISAKMP (0:1): constructed HIS NAT-D *ISAKMP (0:1): constructed MINE NAT-D *ISAKMP (0:1): sending packet to 10.0.0.1 my_port 500 peer_port 500 (R) AG_INIT_EXCH *ISAKMP (0:1): Input = IKE_MESG_FROM_AAA, PRESHARED_KEY_REPLY *ISAKMP

(0:1): Old State = IKE_R_AM_AAA_AWAIT New State = IKE_R_AM2 *AAA/MEMORY: free_user (0x830E12E8) user='3000client' ruser='NULL' port='ISAKMP-ID-AUTH' rem_addr='10.0.0.1' authen_type=NONE service=LOGIN priv=0 vrf= (id=0) *ISAKMP (0:1): received packet from 10.0.0.1 dport 500 sport 500 Global (R) AG_INIT_EXCH *CryptoEng *ISAKMP (0:1): Detected NAT-D payload *ISAKMP (0:1): recalc his hash for NAT-D *ISAKMP (0:1): NAT match HIS hash *ISAKMP (0:1): SA has been authenticated with 10.0.0.1 *CryptoEngine0: clear dh number for conn id 1 *ISAKMP: Trying to insert a peer 10.0.0.1/500/, and inserted successfully. *ISAKMP (0:1): IKE_DPD is enabled, initializing timers *ISAKMP: set new node 2011892843 to CONF_XAUTH *CryptoEngine0: generate hmac context for conn id 1 *CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec) *IPSEC(key_engine): got a queue event... *CryptoEngine0: CRYPTO_ISA_DH_DELETE(hw)(ipsec) *CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec) *ISAKMP (0:1): sending packet to 10.0.0.1 my_port 500 peer_port 500 (R) QM_IDLE *ISAKMP (0:1): purging node 2011892843 *ISAKMP: Sending phase 1 responder lifetime 86400 *ISAKMP (0:1): peer matches *none* of the profiles *ISAKMP (0:1): Input = IKE_MSG_FROM_PEER, IKE_AM_EXCH *ISAKMP (0:1): Old State = IKE_R_AM2 New State = IKE_P1_COMPLETE *ISAKMP (0:1): Need XAUTH *AAA: parse name=ISAKMP idb type=-1 tty=-1 *AAA/MEMORY: create_user (0x830DE43C) user='NULL' ruser='NULL' ds0=0 port='ISAKMP' rem_addr='10.0.0.1' authen_type=ASCII service=LOGIN priv=0 initial_task_id='0', vrf= (id=0) *ISAKMP (0:1): Input = IKE_MSG_INTERNAL, **IKE_PHASE1_COMPLETE** *ISAKMP (0:1): Old State = IKE_P1_COMPLETE New State = IKE_XAUTH_AAA_START_LOGIN_AWAIT *AAA/AUTHEN/START (992119247): port='ISAKMP' list='userauthen' action=LOGIN service=LOGIN *AAA/AUTHEN/START (992119247): found list userauthen *AAA/AUTHEN/START (992119247): Method=radius (radius) *AAA/AUTHEN(992119247): Status=GETUSER *ISAKMP: got callback 1 *ISAKMP: set new node -883516238 to CONF_XAUTH *ISAKMP/xauth: request attribute XAUTH_USER_NAME_V2 *ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD_V2 *CryptoEngine0: generate hmac context for conn id 1 *CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec) *ISAKMP (0:1): initiating peer config to 10.0.0.1. ID = -883516238 *CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec) *ISAKMP (0:1): sending packet to 10.0.0.1 my_port 500 peer_port 500 (R) CONF_XAUTH *ISAKMP (0:1): Input = IKE_MSG_FROM_AAA, IKE_AAA_START_LOGIN *ISAKMP (0:1): Old State = IKE_XAUTH_AAA_START_LOGIN_AWAIT New State = IKE_XAUTH_REQ_SENT *ISAKMP (0:1): retransmitting phase 2 CONF_XAUTH -883516238 ... *ISAKMP (0:1): incrementing error counter on sa: retransmit phase 2 *ISAKMP (0:1): incrementing error counter on sa: retransmit phase 2 *ISAKMP (0:1): retransmitting phase 2 -883516238 CONF_XAUTH *ISAKMP (0:1): sending packet to 10.0.0.1 my_port 500 peer_port 500 (R) CONF_XAUTH *ISAKMP (0:1): received packet from 10.0.0.1 dport 500 sport 500 Global (R) CONF_XAUTH *CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec) *ISAKMP (0:1): processing transaction payload from 10.0.0.1. message ID = -883516238 *CryptoEngine0: generate hmac context for conn id 1 *CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec) *ISAKMP: Config payload REPLY *ISAKMP/xauth: reply attribute XAUTH_USER_NAME_V2 *ISAKMP/xauth: reply attribute XAUTH_USER_PASSWORD_V2 *ISAKMP (0:1): deleting node -883516238 error FALSE reason "done with xauth request/reply exchange" *ISAKMP (0:1): Input = IKE_MSG_FROM_PEER, IKE_CFG_REPLY *ISAKMP (0:1): Old State = IKE_XAUTH_REQ_SENT New State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT *AAA/AUTHEN/CONT (992119247): continue_login (user='(undef)') *AAA/AUTHEN(992119247): Status=GETUSER *AAA/AUTHEN(992119247): Method=radius (radius) *AAA/AUTHEN(992119247): Status=GETPASS *AAA/AUTHEN/CONT (992119247): continue_login (user='cisco') *AAA/AUTHEN(992119247): Status=GETPASS *AAA/AUTHEN(992119247): Method=radius (radius) *RADIUS: Pick NAS IP for u=0x830DE43C tableid=0 cfg_addr=0.0.0.0 best_addr=10.1.1.1 *RADIUS: ustruct sharecount=2 *Radius: radius_port_info() success=0 radius_nas_port=1 *RADIUS(00000000): **Send Access-Request to 172.18.124.96:1645 id 21645/4, len 72** *RADIUS: authenticator F2 7F ED 86 2B D9 80 1F - 74 D7 8F 90 3B EF F0 D5 *RADIUS: NAS-IP-Address [4] 6 10.1.1.1 *RADIUS: NAS-Port-Type [61] 6 Async [0] *RADIUS: User-Name [1] 9 "cisco" *RADIUS: Calling-Station-Id [31] 13 "10.0.0.1" *RADIUS: User-Password [2] 18 * *RADIUS: Retransmit to (172.18.124.96:1645,1646) for id 21645/4 *RADIUS: **Received from id 21645/4 172.18.124.96:1645, Access-Accept, len 62** *RADIUS: authenticator 97 DF CB C8 74 AC 92 D6 - 3B D8 D9 DC 9E 85 94 35 *RADIUS: Framed-IP-Address [8] 6 172.17.8.123 *RADIUS: Class [25] 36 *RADIUS: 43 49 53 43 4F 41 43 53 3A 30 30 30 30 31 38 32 [CISCOACS:0000182] *RADIUS: 62 2F 61 63 31 32 37 63 39 66 2F 74 6E 65 75 62 [b/ac127c9f/cisco] *RADIUS: 65 72 *RADIUS: saved authorization data for user 830DE43C at 830DB5FC *AAA/AUTHEN(992119247): Status=PASS *ISAKMP: got callback 1 *ISAKMP: set new node -1874799558 to CONF_XAUTH *CryptoEngine0: generate hmac context for conn id 1 *CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec) *ISAKMP (0:1): initiating peer config to 10.0.0.1. ID = -1874799558 *CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec) *ISAKMP (0:1): sending packet to 10.0.0.1 my_port 500 peer_port 500 (R) CONF_XAUTH *ISAKMP (0:1): Input = IKE_MSG_FROM_AAA, IKE_AAA_CONT_LOGIN *ISAKMP (0:1): Old State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT New State = IKE_XAUTH_SET_SENT *AAA/MEMORY: free_user (0x830DE43C) user='cisco' ruser='NULL' port='ISAKMP' rem_addr='10.0.0.1' authen_type=ASCII service=LOGIN priv=0 vrf= (id=0) *ISAKMP (0:1): received packet from 10.0.0.1 dport 500 sport 500 Global (R) CONF_XAUTH *CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec) *ISAKMP (0:1): processing transaction payload from 10.0.0.1.

message ID = -1874799558 *CryptoEngine0: generate hmac context for conn id 1 *CryptoEngine0:
CRYPTO_ISA_IKE_HMAC(hw)(ipsec) *ISAKMP: Config payload ACK *ISAKMP (0:1): XAUTH ACK Processed
*ISAKMP (0:1): deleting node -1874799558 error FALSE reason "done with transaction" *ISAKMP
(0:1): Input = IKE_MSG_FROM_PEER, IKE_CFG_ACK *ISAKMP (0:1): Old State = IKE_XAUTH_SET_SENT New
State = IKE_P1_COMPLETE *ISAKMP (0:1): Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE *ISAKMP
(0:1): Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE *ISAKMP (0:1): received packet
from 10.0.0.1 dport 500 sport 500 Global (R) QM_IDLE *ISAKMP: set new node -1474156599 to
QM_IDLE *CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec) *ISAKMP (0:1): processing transaction
payload from 10.0.0.1. message ID = -1474156599 *CryptoEngine0: generate hmac context for conn
id 1 *CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec) *ISAKMP: Config payload REQUEST *ISAKMP
(0:1): checking request: *ISAKMP: IP4_ADDRESS *ISAKMP: IP4_NETMASK *ISAKMP: IP4_DNS *ISAKMP:
IP4_NBNS *ISAKMP: ADDRESS_EXPIRY *ISAKMP: APPLICATION_VERSION *ISAKMP: UNKNOWN Unknown Attr:
0x7000 *ISAKMP: UNKNOWN Unknown Attr: 0x7001 *ISAKMP: DEFAULT_DOMAIN *ISAKMP: SPLIT_INCLUDE
*ISAKMP: UNKNOWN Unknown Attr: 0x7003 *ISAKMP: UNKNOWN Unknown Attr: 0x7007 *ISAKMP: UNKNOWN
Unknown Attr: 0x7008 *ISAKMP: UNKNOWN Unknown Attr: 0x7009 *ISAKMP: UNKNOWN Unknown Attr: 0x700A
*ISAKMP: UNKNOWN Unknown Attr: 0x7005 *AAA: parse name=ISAKMP-GROUP-AUTH idb type=-1 tty=-1
*AAA/MEMORY: create_user (0x831663A0) user='3000client' ruser='NULL' ds0=0 port='ISAKMP-GROUP-
AUTH' rem_addr='10.0.0.1' authn_type=NONE service=LOGIN priv=0 initial_task_id='0', vrf=(id=0)
*ISAKMP (0:1): Input = IKE_MSG_FROM_PEER, IKE_CFG_REQUEST *ISAKMP (0:1): Old State =
IKE_P1_COMPLETE New State = IKE_CONFIG_AUTHOR_AAA_AWAIT *ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO
AAA(3136771130): Port='ISAKMP-GROUP-AUTH' list='groupauthor' service=NET *AAA/AUTHOR/CRYPTO AAA:
ISAKMP-GROUP-AUTH(3136771130) user='3000client' *ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO
AAA(3136771130): send AV service=ike *ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(3136771130): send
AV protocol=ipsec *ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(3136771130): found list "groupauthor"
*ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(3136771130): Method=LOCAL *AAA/AUTHOR (3136771130):
Post authorization status = PASS_ADD *ISAKMP: got callback 1 * AAA/AUTHOR/IKE: Processing AV
service=ike * AAA/AUTHOR/IKE: Processing AV protocol=ipsec * AAA/AUTHOR/IKE: Processing AV
tunnel-password=cisco123 * AAA/AUTHOR/IKE: Processing AV default-domain*cisco.com *
AAA/AUTHOR/IKE: Processing AV addr-pool*ippool * AAA/AUTHOR/IKE: Processing AV key-exchange=ike
* AAA/AUTHOR/IKE: Processing AV group-lock*0 * AAA/AUTHOR/IKE: Processing AV timeout*0 *
AAA/AUTHOR/IKE: Processing AV idletime*0 * AAA/AUTHOR/IKE: Processing AV inacl*108 *
AAA/AUTHOR/IKE: Processing AV dns-servers*10.1.1.10 0.0.0.0 * AAA/AUTHOR/IKE: Processing AV
wins-servers*10.1.1.20 0.0.0.0 *ISAKMP (0:1): attributes sent in message: * Address: 0.2.0.0
*ISAKMP (0:1): allocating address 10.16.20.1 *ISAKMP: Sending private address: 10.16.20.1
*ISAKMP: Sending IP4_DNS server address: 10.1.1.10 *ISAKMP: Sending IP4_NBNS server address:
10.1.1.20 *ISAKMP: Sending ADDRESS_EXPIRY seconds left to use the address: 86388 *ISAKMP:
Sending APPLICATION_VERSION string: Cisco Internetwork Operating System Software IOS (tm) C2600
Software (C2600-IK9S-M), Version 12.2(15)T2, RELEASE SOFTWARE (fc2) TAC Support:
http://www.cisco.com/tac Copyright (c) 1986-2003 by cisco Systems, Inc. Compiled Thu 01-May-03
10:39 by nmasa *ISAKMP (0/1): Unknown Attr: UNKNOWN (0x7000) *ISAKMP (0/1): Unknown Attr:
UNKNOWN (0x7001) *ISAKMP: Sending DEFAULT_DOMAIN default domain name: cisco.com *ISAKMP: Sending
split include name 108 network 172.18.124.0 mask 255.255.255.0 protocol 0, src port 0, dst port
0 *ISAKMP (0/1): Unknown Attr: UNKNOWN (0x7003) *ISAKMP (0/1): Unknown Attr: UNKNOWN (0x7007)
*ISAKMP (0/1): Unknown Attr: UNKNOWN (0x7008) *ISAKMP (0/1): Unknown Attr: UNKNOWN (0x7009)
*ISAKMP (0/1): Unknown Attr: UNKNOWN (0x700A) *ISAKMP (0/1): Unknown Attr: UNKNOWN (0x7005)
*CryptoEngine0: generate hmac context for conn id 1 *CryptoEngine0:
CRYPTO_ISA_IKE_HMAC(hw)(ipsec) *ISAKMP (0:1): responding to peer config from 10.0.0.1. ID = -
1474156599 *CryptoEngi*ISAKMP (0:1): deleting node -1474156599 error FALSE reason ""ne0:
CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec) *ISAKMP (0:1): sending packet to 10.0.0.1 my_por231 *ISAKMP
(0:1): processing SA payload. message ID = 2058744231 *ISAKMP (0:1): Checking IPsec proposal 1
*ISAKMP: transform 1, ESP_AES *ISAKMP: attributes in transform: *ISAKMP: authenticator is HMAC-
MD5 *ISAKMP: encaps is 1 *ISAKMP: key length is 256t 500 peer_port 500 (R) CONF_ADDR *ISAKMP
(0:1): Input = IKE_MSG_FROM_AAA, IKE_AAA_GROUP_ATTR *ISAKMP (0:1): Old State =
IKE_CONFIG_AUTHOR_AAA_AWAIT New State = IKE_P1_COMPLETE *AAA/MEMORY: free_user (0x831663A0)
user='3000client' ruser='NULL' port='ISAKMP-GROUP-AUTH' rem_addr='10.0.0.1' authn_type=NONE
service=LOGIN priv=0 vrf=(id=0) *ISAKMP (0:1): received packet from 10.0.0.1 dport 500 sport
500 Global (R) QM_IDLE *ISAKMP: set new node 2058744231 to QM_IDLE *CryptoEngine0:
CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec) *CryptoEngine0: generate hmac context for conn id 1
*CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec) *ISAKMP (0:1): processing HASH payload. message
ID = 2058744 *ISAKMP: SA life type in seconds *ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4
0x9B *CryptoEngine0: validate proposal *ISAKMP (0:1): atts are acceptable. *ISAKMP (0:1):
Checking IPsec proposal 1 *ISAKMP (0:1): transform 1, IPPCP LZS *ISAKMP: attributes in
transform: *ISAKMP: encaps is 1 *ISAKMP: SA life type in seconds *ISAKMP: SA life duration (VPI)
of 0x0 0x20 0xC4 0x9B *ISAKMP (0:1): atts are acceptable. *IPSEC(validate_proposal_request):

proposal part #1, (key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1, local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-aes 256 esp-md5-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x2 *IPSEC(validate_proposal_request): proposal part #2, (key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1, local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1), protocol= PCP, transform= comp-lzs , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2 *CryptoEngine0: validate proposal request *IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf =
*IPSEC(validate_transform_proposal): transform proposal not supported for identity: {esp-aes 256 esp-md5-hmac comp-lzs } *ISAKMP (0:1): IPsec policy invalidated proposal *ISAKMP (0:1): Checking IPsec proposal 2 *ISAKMP: transform 1, ESP_AES *ISAKMP: attributes in transform: *ISAKMP: authenticator is HMAC-SHA *ISAKMP: encaps is 1 *ISAKMP: key length is 256 *ISAKMP: SA life type in seconds *ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B *CryptoEngine0: validate proposal *ISAKMP (0:1): atts are acceptable. *ISAKMP (0:1): Checking IPsec proposal 2 *ISAKMP (0:1): transform 1, IPPCP LZS *ISAKMP: attributes in transform: *ISAKMP: encaps is 1 *ISAKMP: SA life type in seconds *ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B *ISAKMP (0:1): atts are acceptable. *IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1, local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-aes 256 esp-sha-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x2 *IPSEC(validate_proposal_request): proposal part #2, (key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1, local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1), protocol= PCP, transform= comp-lzs , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2 *CryptoEngine0: validate proposal request *IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf =
*IPSEC(validate_transform_proposal): transform proposal not supported for identity: {esp-aes 256 esp-sha-hmac comp-lzs } *ISAKMP (0:1): IPsec policy invalidated proposal *ISAKMP (0:1): Checking IPsec proposal 3 *ISAKMP: transform 1, ESP_AES *ISAKMP: attributes in transform: *ISAKMP: authenticator is HMAC-MD5 *ISAKMP: encaps is 1 *ISAKMP: key length is 128 *ISAKMP: SA life type in seconds *ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B *CryptoEngine0: validate proposal *ISAKMP (0:1): atts are acceptable. *ISAKMP (0:1): Checking IPsec proposal 3 *ISAKMP (0:1): transform 1, IPPCP LZS *ISAKMP: attributes in transform: *ISAKMP: encaps is 1 *ISAKMP: SA life type in seconds *ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B *ISAKMP (0:1): atts are acceptable. *IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1, local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-aes esp-md5-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x2 *IPSEC(validate_proposal_request): proposal part #2, (key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1, local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1), protocol= PCP, transform= comp-lzs , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2 *CryptoEngine0: validate proposal request *IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf =
*IPSEC(validate_transform_proposal): transform proposal not supported for identity: {esp-aes esp-md5-hmac comp-lzs } *ISAKMP (0:1): IPsec policy invalidated proposal *ISAKMP (0:1): Checking IPsec proposal 4 *ISAKMP: transform 1, ESP_AES *ISAKMP: attributes in transform: *ISAKMP: authenticator is HMAC-SHA *ISAKMP: encaps is 1 *ISAKMP: key length is 128 *ISAKMP: SA life type in seconds *ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B *CryptoEngine0: validate proposal *ISAKMP (0:1): atts are acceptable. *ISAKMP (0:1): Checking IPsec proposal 4 *ISAKMP (0:1): transform 1, IPPCP LZS *ISAKMP: attributes in transform: *ISAKMP: encaps is 1 *ISAKMP: SA life type in seconds *ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B *ISAKMP (0:1): atts are acceptable. *IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1, local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-aes esp-sha-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x2 *IPSEC(validate_proposal_request): proposal part #2, (key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1, local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1), protocol= PCP, transform= comp-lzs , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2 *CryptoEngine0: validate proposal request *IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf =
*IPSEC(validate_transform_proposal): transform proposal not supported for identity: {esp-aes esp-sha-hmac comp-lzs } *ISAKMP (0:1): IPsec policy invalidated proposal *ISAKMP (0:1): Checking IPsec proposal 5 *ISAKMP: transform 1, ESP_AES *ISAKMP: attributes in transform: *ISAKMP: authenticator is HMAC-MD5 *ISAKMP: encaps is 1 *ISAKMP: key length is 256 *ISAKMP: SA life type in seconds *ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B *CryptoEngine0: validate

proposal *ISAKMP (0:1): atts are acceptable. *IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1, local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-aes 256 esp-md5-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x2 *CryptoEngine0: validate proposal request *IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf = *IPSEC(validate_transform_proposal): transform proposal not supported for identity: {esp-aes 256 esp-md5-hmac } *ISAKMP (0:1): IPSec policy invalidated proposal *ISAKMP (0:1): Checking IPSec proposal 6 *ISAKMP: transform 1, ESP_AES *ISAKMP: attributes in transform: *ISAKMP: authenticator is HMAC-SHA *ISAKMP: encaps is 1 *ISAKMP: key length is 256 *ISAKMP: SA life type in seconds *ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B *CryptoEngine0: validate proposal *ISAKMP (0:1): atts are acceptable. *IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1, local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-aes 256 esp-sha-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x2 *CryptoEngine0: validate proposal request *IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf = *IPSEC(validate_transform_proposal): transform proposal not supported for identity: {esp-aes 256 esp-sha-hmac } *ISAKMP (0:1): IPSec policy invalidated proposal *ISAKMP (0:1): Checking IPSec proposal 7 *ISAKMP: transform 1, ESP_AES *ISAKMP: attributes in transform: *ISAKMP: authenticator is HMAC-MD5 *ISAKMP: encaps is 1 *ISAKMP: key length is 128 *ISAKMP: SA life type in seconds *ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B *CryptoEngine0: validate proposal *ISAKMP (0:1): atts are acceptable. *IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1, local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-aes esp-md5-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x2 *CryptoEngine0: validate proposal request *IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf = *IPSEC(validate_transform_proposal): transform proposal not supported for identity: {esp-aes esp-md5-hmac } *ISAKMP (0:1): IPSec policy invalidated proposal *ISAKMP (0:1): Checking IPSec proposal 8 *ISAKMP: transform 1, ESP_AES *ISAKMP: attributes in transform: *ISAKMP: authenticator is HMAC-SHA *ISAKMP: encaps is 1 *ISAKMP: key length is 128 *ISAKMP: SA life type in seconds *ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B *CryptoEngine0: validate proposal *ISAKMP (0:1): atts are acceptable. *IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1, local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-aes esp-sha-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x2 *CryptoEngine0: validate proposal request *IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf = *IPSEC(validate_transform_proposal): transform proposal not supported for identity: {esp-aes esp-sha-hmac } *ISAKMP (0:1): IPSec policy invalidated proposal *ISAKMP (0:1): Checking IPSec proposal 9 *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 *CryptoEngine0: validate proposal *ISAKMP (0:1): atts are acceptable. *ISAKMP (0:1): Checking IPSec proposal 9 *ISAKMP (0:1): transform 1, IPPCP LZS *ISAKMP: attributes in transform: *ISAKMP: encaps is 1 *ISAKMP: SA life type in seconds *IPSEC(spi_response): getting spi 3233689542 for SA from 10.1.1.1 to 10.0.0.1 for prot 3 *ISAKMP: received ke message (2/1) *CryptoEngine0: generate hmac context for conn id 1 *CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec) *CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec) *ISAKMP (0:1): sending packet to 10.0.0.1 my_port 500 peer_port 500 (R) QM_IDLE *ISAKMP (0:1): Node 2058744231, Input = IKE_MSG_FROM_IPSEC, IKE_SPI_REPLY *ISAKMP (0:1): Old State = IKE_QM_SPI_STARVE New State = IKE_QM_R_QM2 *ISAKMP (0:1): received packet from 10.0.0.1 dport 500 sport 500 Global (R) QM_IDLE *CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec) *CryptoEngine0: generate hmac context for conn id 1 *CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec) *CryptoEngine0: ipsec allocate flow *CryptoEngine0: ipsec allocate flow *CryptoEngine0: CRYPTO_ISA_IPSEC_KEY_CREATE(hw)(ipsec) *CryptoEngine0: CRYPTO_ISA_IPSEC_KEY_CREATE(hw)(ipsec) *ISAKMP: Locking peer struct 0x83166B20, IPSEC refcount 1 for for stuff_ke !--- A matching IPSec policy has been negotiated and authenticated. !--- Next, the SA's are set up. *ISAKMP (0:1): Creating IPSec SAs * inbound SA from 10.0.0.1 to 10.1.1.1 (f/i) 0/ 0 (proxy 10.16.20.1 to 10.1.1.1) * has spi 0xC0BE2FC6 and conn_id 420 and flags 2 * lifetime of 2147483 seconds * has client flags 0x0 * outbound SA from 10.1.1.1 to 10.0.0.1 (f/i) 0/ 0 (proxy 10.1.1.1 to 10.16.20.1) *ISAKMP (0:1): received packet from 10.0.0.1 dport 500 sport 500 Global (R) QM_IDLE *ISAKMP: set new node 1101355775 to QM_IDLE *CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec) *CryptoEngine0: generate hmac context for conn id 1 *CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec) *ISAKMP (0:1): processing HASH payload. message ID = 1101355775 *ISAKMP (0:1): processing SA payload. message ID = 1101355775 *ISAKMP (0:1):

Checking IPsec proposal 1 *ISAKMP: transform 1, ESP_AES *ISAKMP: attributes in transform:
*ISAKMP: authenticator is HMAC-MD5 *ISAKMP: encaps is 1 *ISAKMP: key length is 256 *ISAKMP: SA
life type in seconds *ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B *CryptoEngine0:
validate proposal *ISAKMP (0:1): atts are acceptable. *ISAKMP (0:1): Checking IPsec proposal 1
*ISAKMP (0:1): transform 1, IPPCP LZS *ISAKMP: attributes in transform: *ISAKMP: encaps is 1
*ISAKMP: SA life type in seconds *ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B *ISAKMP
(0:1): atts are acceptable. *IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.)
INBOUND local= 10.1.1.1, remote= 10.0.0.1, local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4),
remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-aes 256
esp-md5-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x2
*IPSEC(validate_proposal_request): proposal part #2, (key eng. msg.) INBOUND local= 10.1.1.1,
remote= 10.0.0.1, local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4), remote_proxy=
10.16.20.1/255.255.255.255/0/0 (type=1), protocol= PCP, transform= comp-lzs , lifedur= 0s and
0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2 *CryptoEngine0: validate proposal request
*IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf = *IPSEC(kei_proxy): head =
clientmap, map->ivrf = , kei->ivrf = *IPSEC(validate_transform_proposal): transform proposal not
supported for identity: {esp-aes 256 esp-md5-hmac comp-lzs } *ISAKMP (0:1): IPsec policy
invalidated proposal *ISAKMP (0:1): Checking IPsec proposal 2 *ISAKMP: transform 1, ESP_AES
*ISAKMP: attributes in transform: *ISAKMP: authenticator is HMAC-SHA *ISAKMP: encaps is 1
*ISAKMP: key length is 256 *ISAKMP: SA life type in seconds *ISAKMP: SA life duration (VPI) of
0x0 0x20 0xC4 0x9B *CryptoEngine0: validate proposal *ISAKMP (0:1): atts are acceptable. *ISAKMP
(0:1): Checking IPsec proposal 2 *ISAKMP (0:1): transform 1, IPPCP LZS *ISAKMP: attributes in
transform: *ISAKMP: encaps is 1 *ISAKMP: SA life type in seconds *ISAKMP: SA life duration (VPI)
of 0x0 0x20 0xC4 0x9B *ISAKMP (0:1): atts are acceptable. *IPSEC(validate_proposal_request):
proposal part #1, (key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1, local_proxy=
172.18.124.0/255.255.255.0/0/0 (type=4), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-aes 256 esp-sha-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id=
0, keysize= 256, flags= 0x2 *IPSEC(validate_proposal_request): proposal part #2, (key eng. msg.)
INBOUND local= 10.1.1.1, remote= 10.0.0.1, local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4),
remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1), protocol= PCP, transform= comp-lzs ,
lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2 *CryptoEngine0: validate
proposal request *IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf =
*IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf =
*IPSEC(validate_transform_proposal): transform proposal not supported for identity: {esp-aes 256
esp-sha-hmac comp-lzs } *ISAKMP (0:1): IPsec policy invalidated proposal *ISAKMP (0:1): Checking
IPsec proposal 3 *ISAKMP: transform 1, ESP_AES *ISAKMP: attributes in transform: *ISAKMP:
authenticator is HMAC-MD5 *ISAKMP: encaps is 1 *ISAKMP: key length is 128 *ISAKMP: SA life type
in seconds *ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B *CryptoEngine0: validate
proposal *ISAKMP (0:1): atts are acceptable. *ISAKMP (0:1): Checking IPsec proposal 3 *ISAKMP
(0:1): transform 1, IPPCP LZS *ISAKMP: attributes in transform: *ISAKMP: encaps is 1 *ISAKMP: SA
life type in seconds *ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B *ISAKMP (0:1): atts
are acceptable. *IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND
local= 10.1.1.1, remote= 10.0.0.1, local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4),
remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-aes esp-
md5-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x2
*IPSEC(validate_proposal_request): proposal part #2, (key eng. msg.) INBOUND local= 10.1.1.1,
remote= 10.0.0.1, local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4), remote_proxy=
10.16.20.1/255.255.255.255/0/0 (type=1), protocol= PCP, transform= comp-lzs , lifedur= 0s and
0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2 *CryptoEngine0: validate proposal request
*IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf = *IPSEC(kei_proxy): head =
clientmap, map->ivrf = , kei->ivrf = *IPSEC(validate_transform_proposal): transform proposal not
supported for identity: {esp-aes esp-md5-hmac comp-lzs } *ISAKMP (0:1): IPsec policy invalidated
proposal *ISAKMP (0:1): Checking IPsec proposal 4 *ISAKMP: transform 1, ESP_AES *ISAKMP:
attributes in transform: *ISAKMP: authenticator is HMAC-SHA *ISAKMP: encaps is 1 *ISAKMP: key
length is 128 *ISAKMP: SA life type in seconds *ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4
0x9B *CryptoEngine0: validate proposal *ISAKMP (0:1): atts are acceptable. *ISAKMP (0:1):
Checking IPsec proposal 4 *ISAKMP (0:1): transform 1, IPPCP LZS *ISAKMP: attributes in
transform: *ISAKMP: encaps is 1 *ISAKMP: SA life type in seconds *ISAKMP: SA life duration (VPI)
of 0x0 0x20 0xC4 0x9B *ISAKMP (0:1): atts are acceptable. *IPSEC(validate_proposal_request):
proposal part #1, (key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1, local_proxy=
172.18.124.0/255.255.255.0/0/0 (type=4), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-aes esp-sha-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0,
keysize= 128, flags= 0x2 *IPSEC(validate_proposal_request): proposal part #2, (key eng. msg.)
INBOUND local= 10.1.1.1, remote= 10.0.0.1, local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4),


```
remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1), protocol= PCP, transform= comp-lzs ,
lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2 *CryptoEngine0: validate
proposal request *IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf =
*IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf =
*IPSEC(validate_transform_proposal): transform proposal not supported for identity: {esp-aes
esp-sha-hmac comp-lzs } *ISAKMP (0:1): IPsec policy invalidated proposal *ISAKMP (0:1): Checking
IPsec proposal 5 *ISAKMP: transform 1, ESP_AES *ISAKMP: attributes in transform: *ISAKMP:
authenticator is HMAC-MD5 *ISAKMP: encaps is 1 *ISAKMP: key length is 256 *ISAKMP: SA life type
in seconds *ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B *CryptoEngine0: validate
proposal *ISAKMP (0:1): atts are acceptable. *IPSEC(validate_proposal_request): proposal part
#1, (key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1, local_proxy=
172.18.124.0/255.255.255.0/0/0 (type=4), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-aes 256 esp-md5-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id=
0, keysize= 256, flags= 0x2 *CryptoEngine0: validate proposal request *IPSEC(kei_proxy): head =
clientmap, map->ivrf = , kei->ivrf = *IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei-
>ivrf = *IPSEC(validate_transform_proposal): transform proposal not supported for identity:
{esp-aes 256 esp-md5-hmac } *ISAKMP (0:1): IPsec policy invalidated proposal *ISAKMP (0:1):
Checking IPsec proposal 6 *ISAKMP: transform 1, ESP_AES *ISAKMP: attributes in transform:
*ISAKMP: authenticator is HMAC-SHA *ISAKMP: encaps is 1 *ISAKMP: key length is 256 *ISAKMP: SA
life type in seconds *ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B *CryptoEngine0:
validate proposal *ISAKMP (0:1): atts are acceptable. *IPSEC(validate_proposal_request):
proposal part #1, (key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1, local_proxy=
172.18.124.0/255.255.255.0/0/0 (type=4), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-aes 256 esp-sha-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id=
0, keysize= 256, flags= 0x2 *CryptoEngine0: validate proposal request *IPSEC(kei_proxy): head =
clientmap, map->ivrf = , kei->ivrf = *IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei-
>ivrf = *IPSEC(validate_transform_proposal): transform proposal not supported for identity:
{esp-aes 256 esp-sha-hmac } *ISAKMP (0:1): IPsec policy invalidated proposal *ISAKMP (0:1):
Checking IPsec proposal 7 *ISAKMP: transform 1, ESP_AES *ISAKMP: attributes in transform:
*ISAKMP: authenticator is HMAC-MD5 *ISAKMP: encaps is 1 *ISAKMP: key length is 128 *ISAKMP: SA
life type in seconds *ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B *CryptoEngine0:
validate proposal *ISAKMP (0:1): atts are acceptable. *IPSEC(validate_proposal_request):
proposal part #1, (key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1, local_proxy=
172.18.124.0/255.255.255.0/0/0 (type=4), remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-aes esp-md5-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0,
keysize= 128, flags= 0x2 *CryptoEngine0: validate proposal request *IPSEC(kei_proxy): head =
clientmap, map->ivrf = , kei->ivrf = *IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei-
>ivrf = *IPSEC(validate_transform_proposal): transform proposal not supported for identity:
{esp-aes esp-md5-hmac } *ISAKMP (0:1): IPsec policy invalidated proposal *ISAKMP (0:1): Checking
IPsec proposal 8 *ISAKMP: transform 1, ESP_AES *ISAKMP: attributes in transform: *ISAKMP:
authenticator is HMAC-SHA *ISAKMP: encaps is 1 *ISAKMP: key length is 128 *ISAKMP: SA life type
in seconds *ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B *CryptoEngine0: validate
proposal *ISAKMP (0:1): atts are acceptable. *IPSEC(spi_response): getting spi 3438126624 for SA
from 10.1.1.1 to 10.0.0.1 for prot 3 *ISAKMP: received ke message (2/1) *CryptoEngine0: generate
hmac context for conn id 1 *CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec) *CryptoEngine0:
CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec) *ISAKMP (0:1): sending packet to 10.0.0.1 my_port 500
peer_port 500 (R) QM_IDLE *ISAKMP (0:1): Node 1101355775, Input = IKE_MSG_FROM_IPSEC,
IKE_SPI_REPLY *ISAKMP (0:1): Old State = IKE_QM_SPI_STARVE New State = IKE_QM_R_QM2 *ISAKMP
(0:1): received packet from 10.0.0.1 dport 500 sport 500 Global (R) QM_IDLE *CryptoEngine0:
CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec) *CryptoEngine0: generate hmac context for conn id 1
*CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec) *CryptoEngine0: ipsec allocate flow
*CryptoEngine0: ipsec allocate flow *CryptoEngine0: CRYPTO_ISA_IPSEC_KEY_CREATE(hw)(ipsec)
*CryptoEngine0: CRYPTO_ISA_IPSEC_KEY_CREATE(hw)(ipsec) *ISAKMP: Locking peer struct 0x83166B20,
IPSEC refcount 2 for for stuff_ke *ISAKMP (0:1): Creating IPsec SAs * inbound SA from 10.0.0.1
to 10.1.1.1 (f/i) 0/ 0 (proxy 10.16.20.1 to 172.18.124.0) * has spi 0xCCEDA620 and conn_id 422
and flags 2 * lifetime of 2147483 seconds * has client flags 0x0 * outbound SA from 10.1.1.1 to
10.0.0.1 (f/i) 0/ 0 (proxy 172.18.124.0 to 10.16.20.1 )
```

[クライアント ログ](#)

ログを表示するには、VPN Client で LogViewer を起動します。設定済みのクラスすべてに対してフィルタが High に設定されていることを確認してください。次に、サンプルのログ出力を示します。

1 16:52:27.031 06/18/03 Sev=Info/6 DIALER/0x63300002
Initiating connection.

2 16:52:27.041 06/18/03 Sev=Info/4 CM/0x63100002
Begin connection process

3 16:52:27.051 06/18/03 Sev=Info/4 CM/0x63100004
Establish secure connection using Ethernet

4 16:52:27.051 06/18/03 Sev=Info/4 CM/0x63100024
Attempt connection with server "10.1.1.1"

5 16:52:27.101 06/18/03 Sev=Info/6 IKE/0x6300003B
Attempting to establish a connection with 10.1.1.1.

6 16:52:27.481 06/18/03 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK AG (SA, KE, NON, ID, VID, VID, VID, VID, VID)
to 10.1.1.1

7 16:52:27.612 06/18/03 Sev=Info/4 IPSEC/0x63700014
Deleted all keys

8 16:52:27.722 06/18/03 Sev=Info/5 IKE/0x6300002F
Received ISAKMP packet: peer = 10.1.1.1

9 16:52:27.722 06/18/03 Sev=Info/4 IKE/0x63000014
RECEIVING <<< ISAKMP OAK AG (SA, VID, VID, VID, VID, VID, KE, ID, NON, HASH, NAT-D, NAT-D)
from 10.1.1.1

10 16:52:27.722 06/18/03 Sev=Info/5 IKE/0x63000059
Vendor ID payload = 12F5F28C457168A9702D9FE274CC0100

11 16:52:27.722 06/18/03 Sev=Info/5 IKE/0x63000001
Peer is a Cisco-Unity compliant peer

12 16:52:27.722 06/18/03 Sev=Info/5 IKE/0x63000059
Vendor ID payload = AFCAD71368A1F1C96B8696FC77570100

13 16:52:27.722 06/18/03 Sev=Info/5 IKE/0x63000001
Peer supports DPD

14 16:52:27.722 06/18/03 Sev=Info/5 IKE/0x63000059
Vendor ID payload = 4F6CF9393C7749D894C6C92D2131AE04

15 16:52:27.722 06/18/03 Sev=Info/5 IKE/0x63000059
Vendor ID payload = 09002689DFD6B712

16 16:52:27.722 06/18/03 Sev=Info/5 IKE/0x63000001
Peer supports XAUTH

17 16:52:27.722 06/18/03 Sev=Info/5 IKE/0x63000059
Vendor ID payload = 90CB80913EBB696E086381B5EC427B1F

18 16:52:27.722 06/18/03 Sev=Info/5 IKE/0x63000001
Peer supports NAT-T

19 16:52:27.782 06/18/03 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK AG *(HASH, NOTIFY:STATUS_INITIAL_CONTACT, NAT-D, NAT-D)
to 10.1.1.1

20 16:52:27.822 06/18/03 Sev=Info/5 IKE/0x6300002F
Received ISAKMP packet: peer = 10.1.1.1

21 16:52:27.822 06/18/03 Sev=Info/4 IKE/0x63000014

RECEIVING <<< ISAKMP OAK INFO *(HASH, NOTIFY:STATUS_RESP_LIFETIME)
from 10.1.1.1

22 16:52:27.822 06/18/03 Sev=Info/5 IKE/0x63000044
RESPONDER-LIFETIME notify has value of 86400 seconds

23 16:52:27.822 06/18/03 Sev=Info/5 IKE/0x63000046
This SA has already been alive for 0 seconds, setting expiry to 86400 seconds from now

24 16:52:27.842 06/18/03 Sev=Info/5 IKE/0x6300002F
Received ISAKMP packet: peer = 10.1.1.1

25 16:52:27.842 06/18/03 Sev=Info/4 IKE/0x63000014
RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 10.1.1.1

26 16:52:27.842 06/18/03 Sev=Info/4 CM/0x63100015
Launch xAuth application

27 16:52:32.449 06/18/03 Sev=Info/5 IKE/0x6300002F
Received ISAKMP packet: peer = 10.1.1.1

28 16:52:32.449 06/18/03 Sev=Info/4 IKE/0x63000014
RECEIVING <<< ISAKMP OAK TRANS *(Retransmission) from 10.1.1.1

29 16:52:32.809 06/18/03 Sev=Info/4 CM/0x63100017
xAuth application returned

30 16:52:32.809 06/18/03 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 10.1.1.1

31 16:52:37.626 06/18/03 Sev=Info/5 IKE/0x6300002F
Received ISAKMP packet: peer = 10.1.1.1

32 16:52:37.636 06/18/03 Sev=Info/4 IKE/0x63000014
RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 10.1.1.1

33 16:52:37.636 06/18/03 Sev=Info/5 IKE/0x63000071
Automatic NAT Detection Status:
Remote end is NOT behind a NAT device
This end is NOT behind a NAT device

34 16:52:37.636 06/18/03 Sev=Info/4 CM/0x6310000E
Established Phase 1 SA. 1 Phase 1 SA in the system

35 16:52:37.656 06/18/03 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 10.1.1.1

36 16:52:37.987 06/18/03 Sev=Info/5 IKE/0x6300005D
Client sending a firewall request to concentrator

37 16:52:37.987 06/18/03 Sev=Info/5 IKE/0x6300005C
Firewall Policy: Product=Cisco Integrated Client, Capability=
(Centralized Protection Policy).

38 16:52:38.007 06/18/03 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 10.1.1.1

39 16:52:38.087 06/18/03 Sev=Info/5 IKE/0x6300002F
Received ISAKMP packet: peer = 10.1.1.1

40 16:52:38.087 06/18/03 Sev=Info/4 IKE/0x63000014
RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 10.1.1.1

41 16:52:38.097 06/18/03 Sev=Info/5 IKE/0x63000010

MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_ADDRESS: , value = 10.16.20.1

42 16:52:38.097 06/18/03 Sev=Info/5 IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_DNS(1): , value = 10.1.1.10

43 16:52:38.097 06/18/03 Sev=Info/5 IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_NBNS(1) (a.k.a. WINS) : , value = 10.1.1.20

44 16:52:38.097 06/18/03 Sev=Info/5 IKE/0xA3000017
MODE_CFG_REPLY: The received (INTERNAL_ADDRESS_EXPIRY) attribute and value (86388)
is not supported

45 16:52:38.097 06/18/03 Sev=Info/5 IKE/0x6300000E
MODE_CFG_REPLY: Attribute = APPLICATION_VERSION, value = Cisco Internetwork
Operating System Software IOS (tm) C2600 Software (C2600-IK9S-M), Version 12.2(15)T2,
RELEASE SOFTWARE (fc2)
TAC Support: <http://www.cisco.com/tac>
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Thu 01-May-03 10:39 by nmasa

46 16:52:38.097 06/18/03 Sev=Info/5 IKE/0x6300000E
MODE_CFG_REPLY: Attribute = MODECFG_UNITY_DEFDOMAIN: , value = cisco.com

47 16:52:38.097 06/18/03 Sev=Info/5 IKE/0x6300000D
MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SPLIT_INCLUDE (# of split_nets),
value = 0x00000001

48 16:52:38.097 06/18/03 Sev=Info/5 IKE/0x6300000F
SPLIT_NET #1
subnet = 172.18.124.0
mask = 255.255.255.0
protocol = 0
src port = 0
dest port=0

49 16:52:38.097 06/18/03 Sev=Info/4 CM/0x63100019
Mode Config data received

50 16:52:38.347 06/18/03 Sev=Info/5 IKE/0x63000055
Received a key request from Driver for IP address 10.1.1.1,
GW IP = 10.1.1.1

51 16:52:38.347 06/18/03 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 10.1.1.1

52 16:52:38.728 06/18/03 Sev=Info/5 IKE/0x6300002F
Received ISAKMP packet: peer = 10.1.1.1

53 16:52:38.728 06/18/03 Sev=Info/4 IKE/0x63000014
RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID, NOTIFY:STATUS_RESP_LIFETIME)
from 10.1.1.1

54 16:52:38.738 06/18/03 Sev=Info/5 IKE/0x63000044
RESPONDER-LIFETIME notify has value of 3600 seconds

55 16:52:38.738 06/18/03 Sev=Info/5 IKE/0x63000045
RESPONDER-LIFETIME notify has value of 4608000 kb

56 16:52:38.738 06/18/03 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK QM *(HASH) to 10.1.1.1

57 16:52:38.738 06/18/03 Sev=Info/5 IKE/0x63000058
Loading IPsec SA (Message ID = 0x7AB5F1A7 OUTBOUND SPI = 0xC0BE2FC6
INBOUND SPI = 0x56FFC535)

58 16:52:38.788 06/18/03 Sev=Info/5 IKE/0x63000025
Loaded OUTBOUND ESP SPI: 0xC0BE2FC6

59 16:52:38.798 06/18/03 Sev=Info/5 IKE/0x63000026
Loaded INBOUND ESP SPI: 0x56FFC535

60 16:52:38.798 06/18/03 Sev=Info/4 CM/0x6310001A
One secure connection established

61 16:52:38.828 06/18/03 Sev=Info/6 DIALER/0x63300003
Connection established.

62 16:52:38.868 06/18/03 Sev=Info/6 CVPND/0x63400011
Found matching adapter

63 16:52:38.968 06/18/03 Sev=Info/6 CVPND/0x63400011
Found matching adapter

64 16:52:39.819 06/18/03 Sev=Info/4 CM/0x63100037
Address watch added for 10.0.0.1. Current address(es): 10.0.0.1.

65 16:52:40.280 06/18/03 Sev=Info/4 IPSEC/0x63700014
Deleted all keys

66 16:52:40.280 06/18/03 Sev=Info/4 IPSEC/0x63700010
Created a new key structure

67 16:52:40.290 06/18/03 Sev=Info/4 IPSEC/0x6370000F
Added key with SPI=0xc62fbec0 into key list

68 16:52:40.290 06/18/03 Sev=Info/4 IPSEC/0x63700010
Created a new key structure

69 16:52:40.290 06/18/03 Sev=Info/4 IPSEC/0x6370000F
Added key with SPI=0x35c5ff56 into key list

70 16:52:41.562 06/18/03 Sev=Info/6 DIALER/0x63300008
MAPI32 Information - Outlook not default mail client

71 16:52:54.230 06/18/03 Sev=Info/5 IKE/0x63000055
Received a key request from Driver for IP address 1.1.1.2, GW IP = 10.1.1.1

72 16:52:54.250 06/18/03 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 10.1.1.1

73 16:52:54.731 06/18/03 Sev=Info/5 IKE/0x6300002F
Received ISAKMP packet: peer = 10.1.1.1

74 16:52:54.731 06/18/03 Sev=Info/4 IKE/0x63000014
RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID, NOTIFY:STATUS_RESP_LIFETIME)
from 10.1.1.1

75 16:52:54.741 06/18/03 Sev=Info/5 IKE/0x63000044
RESPONDER-LIFETIME notify has value of 3600 seconds

76 16:52:54.741 06/18/03 Sev=Info/5 IKE/0x63000045
RESPONDER-LIFETIME notify has value of 4608000 kb

77 16:52:54.741 06/18/03 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK QM *(HASH) to 10.1.1.1

78 16:52:54.741 06/18/03 Sev=Info/5 IKE/0x63000058
Loading IPsec SA (Message ID = 0x41A55AFF OUTBOUND SPI = 0xCCEDA620

INBOUND SPI = 0x0C5B3DB2)

```
79      16:52:54.771  06/18/03  Sev=Info/5      IKE/0x63000025
Loaded OUTBOUND ESP SPI: 0xCCEDA620

80      16:52:54.781  06/18/03  Sev=Info/5      IKE/0x63000026
Loaded INBOUND ESP SPI: 0x0C5B3DB2

81      16:52:54.781  06/18/03  Sev=Info/4      CM/0x63100021
Additional Phase 2 SA established.

82      16:52:55.472  06/18/03  Sev=Info/4      IPSEC/0x63700010
Created a new key structure

83      16:52:55.472  06/18/03  Sev=Info/4      IPSEC/0x6370000F
Added key with SPI=0x20a6edcc into key list

84      16:52:55.472  06/18/03  Sev=Info/4      IPSEC/0x63700010
Created a new key structure

85      16:52:55.472  06/18/03  Sev=Info/4      IPSEC/0x6370000F
Added key with SPI=0xb23d5b0c into key list

86      16:52:55.472  06/18/03  Sev=Info/4      IPSEC/0x63700019
Activate outbound key with SPI=0x20a6edcc for inbound key with SPI=0xb23d5b0c
```

[関連情報](#)

- [RADIUS テクノロジーに関するサポート ページ](#)
- [IPSec ネゴシエーション/IKE プロトコルに関するサポート ページ](#)
- [Cisco VPN Client に関するサポート 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](#)