

2 台のルータと Cisco VPN Client 4.x 間の IPSec の設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[確認](#)

[Cisco VPN 2611](#)

[Cisco VPN 3640](#)

[クリプト マップのシーケンス番号の確認](#)

[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](#)

[関連情報](#)

概要

このドキュメントでは、2 台の Cisco ルータと Cisco VPN Client 4.x 間での IPSec の設定方法について説明します。Cisco IOS® ソフトウェア リリース 12.2(8)T 以降では、Cisco VPN Client 3.x 以降からの接続がサポートされています。

L2Lトンネルの一方の端がもう一方の端でIPアドレスを動的に割り当てられるシナリオについての詳細は、『[IPSecルータのダイナミックLAN-to-LANピアおよびVPN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
- VPN Client用の事前共有キーがcisco123である3000 clientsというグループ
- VPN クライアントに対するグループおよびユーザ認証は、ルータでローカルに実行されること。
- no-xauth パラメータが、LAN-to-LAN トンネルに対する ISAKMP key コマンドで使用されて

いること。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco IOS ソフトウェア リリース 12.2(8)T が稼働しているルータ。注：このドキュメントは、最近、Cisco IOSソフトウェアリリース12.3(1)でテストされました。変更は不要です。
- Cisco VPN Client for Windows バージョン 4.x (VPN Client 3.x 以上であれば正常に動作します)。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

ルータ上で実行された show version コマンドの出力を次に示します。

```
vpn2611#show version
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-JK9O3S-M), Version 12.2(8)T,
  RELEASE SOFTWARE (fc2)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Thu 14-Feb-02 16:50 by ccai
Image text-base: 0x80008070, data-base: 0x81816184

ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)

vpn2611 uptime is 1 hour, 15 minutes
System returned to ROM by reload
System image file is "flash:c2600-jk9o3s-mz.122-8.T"

cisco 2611 (MPC860) processor (revision 0x203)
  with 61440K/4096K bytes of memory.
Processor board ID JAD04370EEG (2285146560)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software (copyright 1990 by Meridian Technology Corp).
TN3270 Emulation software.
2 Ethernet/IEEE 802.3 interface(s)
1 Serial network interface(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102
```

表記法

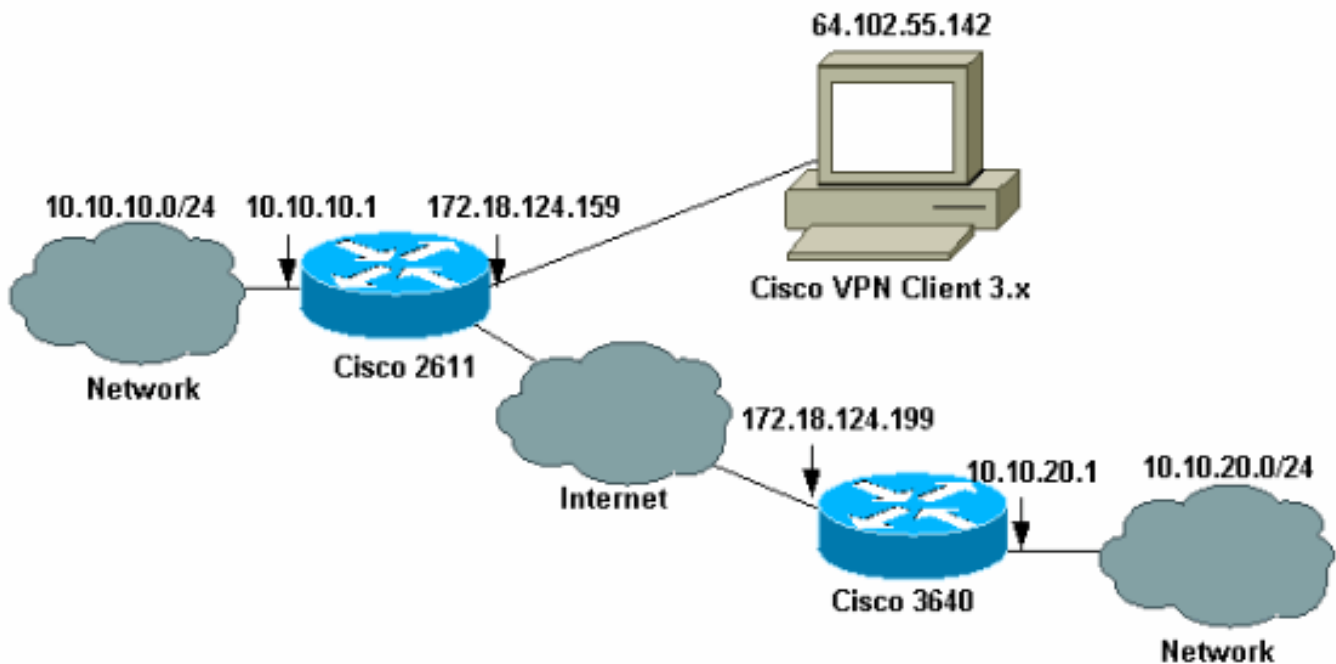
ドキュメント表記の詳細については、『[シスコテクニカルティップスの表記法](#)』を参照してください。

設定

ここでは、このドキュメントで説明する機能の設定に使用する情報を提供します。

ネットワーク図

このドキュメントでは、次のネットワーク設定を使用します。



注：この例のIPアドレスは、ラボネットワークのプライベートIPアドレスであるため、グローバルインターネットではルーティングできません。

設定

Cisco 2611 ルータの設定

Cisco 2611 ルータ

```
vpn2611#show run
Building configuration...

Current configuration : 2265 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname vpn2611
!
!---- Enable AAA for user authentication !---- and group
authorization. aaa new-model
!
!
!---- In order to enable X-Auth for user authentication,
!---- enable the aaa authentication commands.

aaa authentication login userauthen local

!---- In order to enable group authorization, enable !----
```

the **aaa authorization** commands.

```
aaa authorization network groupauthor local
aaa session-id common
!
!--- For local authentication of the IPSec user, !---
create the user with a password. username cisco password
0 cisco
ip subnet-zero
!
!
!
ip audit notify log
ip audit po max-events 100
!
!--- Create an Internet Security Association and !---
Key Management Protocol (ISAKMP) !--- policy for Phase 1
negotiations for the VPN 3.x Clients. crypto isakmp
policy 3
encr 3des
authentication pre-share
group 2
!
!--- Create an ISAKMP policy for Phase 1 !---
negotiations for the LAN-to-LAN tunnels. crypto isakmp
policy 10
hash md5
authentication pre-share
!--- Specify the PreShared key for the LAN-to-LAN
tunnel. !--- Make sure that you use the !--- no-xauth
parameter with your ISAKMP key.
crypto isakmp key cisco123 address 172.18.124.199 no-
xauth
!
!--- Create a group that is used to !--- specify the
WINS, DNS servers' address !--- to the client, along
with the pre-shared !--- key for authentication. crypto
isakmp client configuration group 3000client
key cisco123
dns 10.10.10.10
wins 10.10.10.20
domain cisco.com
pool ippool
!
!
!--- Create the Phase 2 Policy for actual data
encryption. crypto ipsec transform-set myset esp-3des
esp-md5-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. Also create a
new instance for your !--- LAN-to-LAN tunnel. Specify
the peer IP address, !--- transform set, and an Access
Control List (ACL) for this !--- instance. crypto map
clientmap client authentication list userauthen
crypto map clientmap isakmp authorization list
groupauthor
crypto map clientmap client configuration address
respond
crypto map clientmap 1 ipsec-isakmp
set peer 172.18.124.199
set transform-set myset
match address 100
crypto map clientmap 10 ipsec-isakmp dynamic dynmap
!
!
fax interface-type fax-mail
mta receive maximum-recipients 0
!
!
!--- Apply the crypto map on the outside interface.

interface Ethernet0/0
ip address 172.18.124.159 255.255.255.0
half-duplex
crypto map clientmap
!
interface Serial0/0
no ip address
shutdown
!
interface Ethernet0/1
ip address 10.10.10.1 255.255.255.0
no keepalive
half-duplex
!
!
!--- Create a pool of addresses to be !--- assigned to
the VPN Clients. ip local pool ippool 14.1.1.100
14.1.1.200
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.124.1
ip http server
ip pim bidir-enable
!
!
!--- Create an ACL for the traffic !--- to be encrypted.
In this example, !--- the traffic from 10.10.10.0/24 to
10.10.20.0/24 !--- is encrypted. access-list 100 permit
ip 10.10.10.0 0.0.0.255 10.10.20.0 0.0.0.255
!
!
snmp-server community foobar RO
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!

```

```
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
!
!
end
```

[3640 ルータの設定](#)

Cisco 3640 ルータ

```
vpn3640#show run
Building configuration...

Current configuration : 1287 bytes
!
! Last configuration change at 13:47:37 UTC Wed Mar 6
2002
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname vpn3640
!
!
ip subnet-zero
ip cef
!
!---- Create an ISAKMP policy for Phase 1 !----
negotiations for the LAN-to-LAN tunnels. crypto isakmp
policy 10
hash md5
authentication pre-share

!---- Specify the PreShared key for the LAN-to-LAN !----
tunnel. You do not have to add the !--- X-Auth
parameter, as this !--- router does not do Cisco Unity
Client IPsec !--- authentication.

crypto isakmp key cisco123 address 172.18.124.159
!
!

!---- Create the Phase 2 Policy for actual data
encryption. crypto ipsec transform-set myset esp-3des
esp-md5-hmac
!

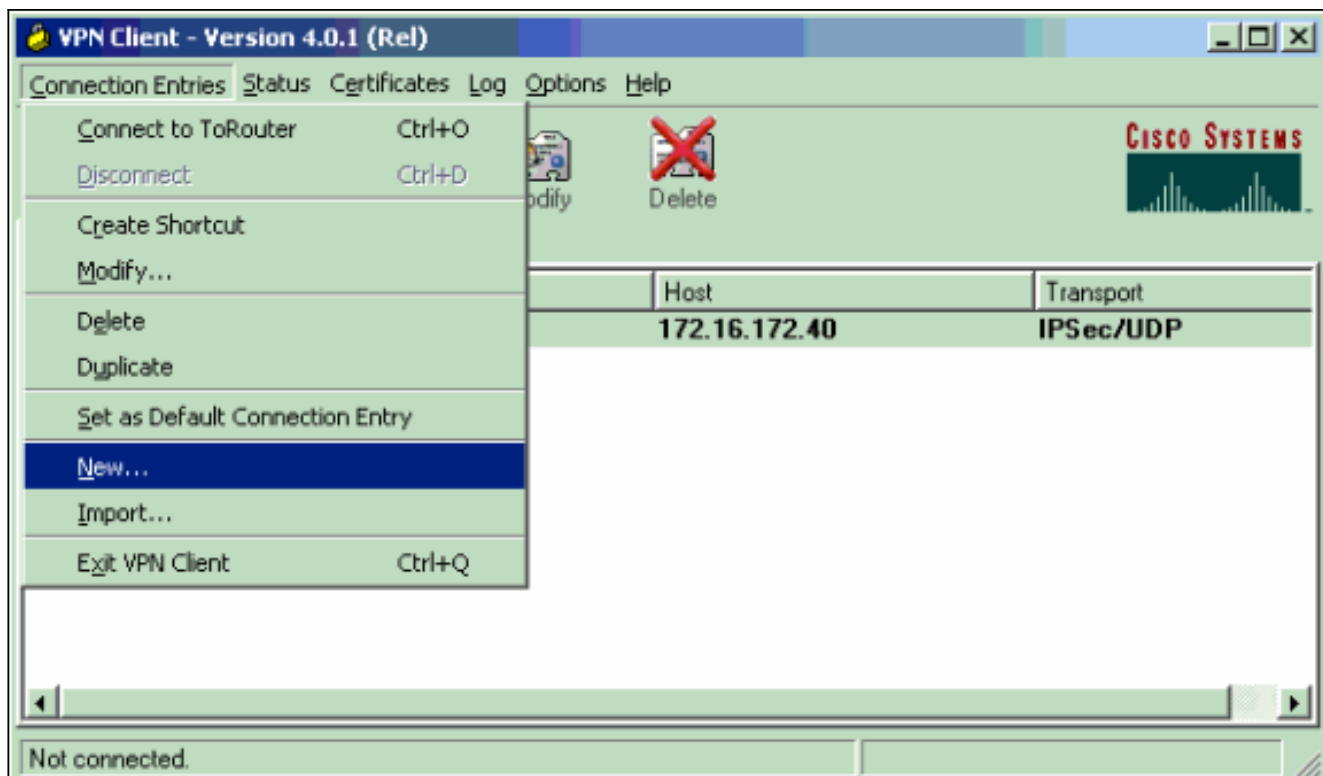
!---- Create the actual crypto map. Specify !---- the peer
IP address, transform !---- set, and an ACL for this
instance. crypto map mymap 10 ipsec-isakmp
set peer 172.18.124.159
set transform-set myset
match address 100
!
call RSVP-sync
!
!
```

```
!  
  
!--- Apply the crypto map on the outside interface.  
interface Ethernet0/0  
ip address 172.18.124.199 255.255.255.0  
half-duplex  
crypto map mymap  
!  
interface Ethernet0/1  
ip address 10.10.20.1 255.255.255.0  
half-duplex  
!  
ip classless  
ip route 0.0.0.0 0.0.0.0 172.18.124.1  
ip http server  
ip pim bidir-enable  
!  
  
!--- Create an ACL for the traffic to !--- be encrypted.  
In this example, !--- the traffic from 10.10.20.0/24 to  
10.10.10.0/24 !--- is encrypted. access-list 100 permit  
ip 10.10.20.0 0.0.0.255 10.10.10.0 0.0.0.255  
snmp-server community foobar RO  
!  
dial-peer cor custom  
!  
!  
line con 0  
exec-timeout 0 0  
line aux 0  
line vty 0 4  
login  
!  
end
```

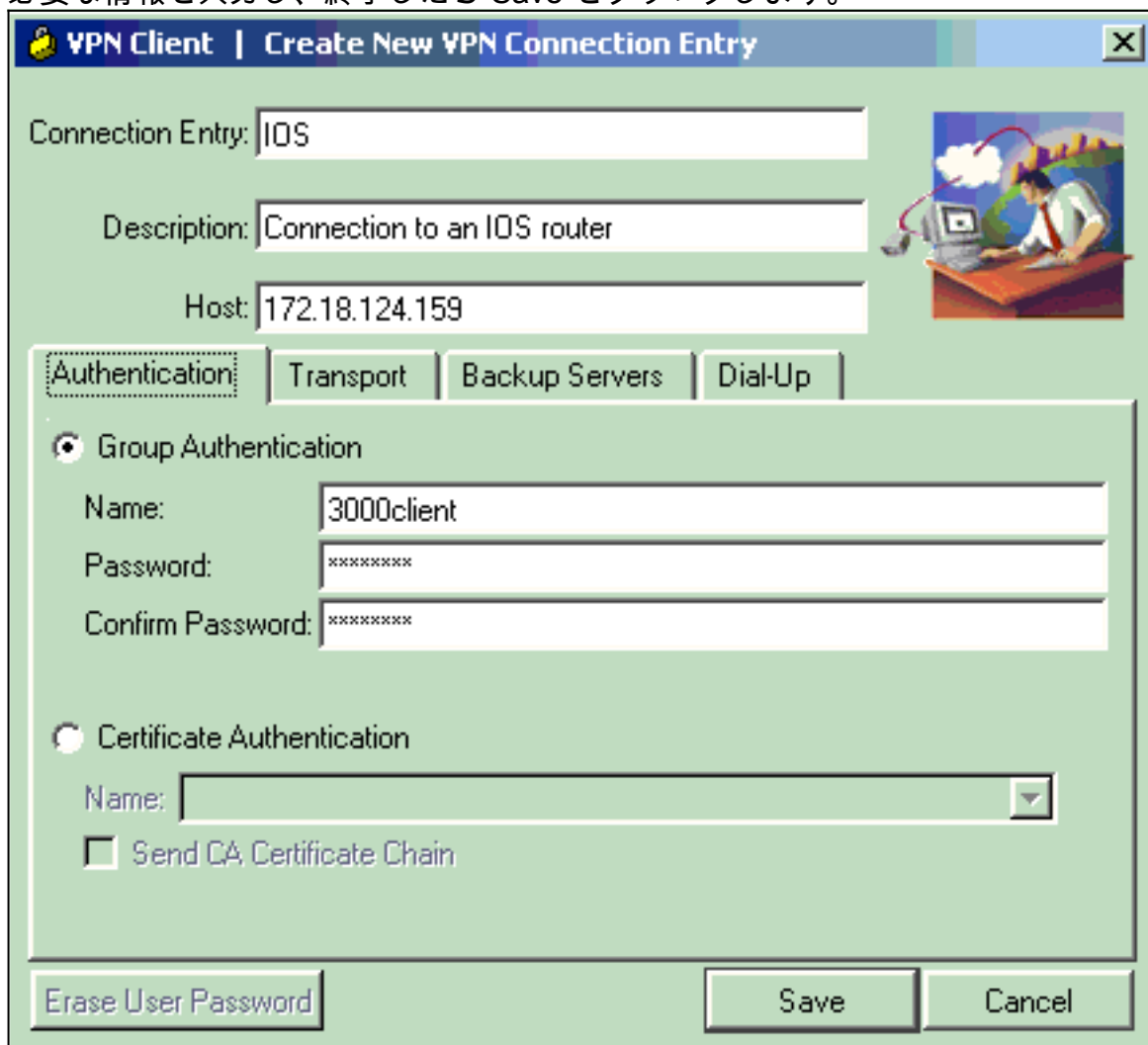
VPN Client 4.x の設定

Cisco VPN Client 4.x を設定するには、次の手順に従います。

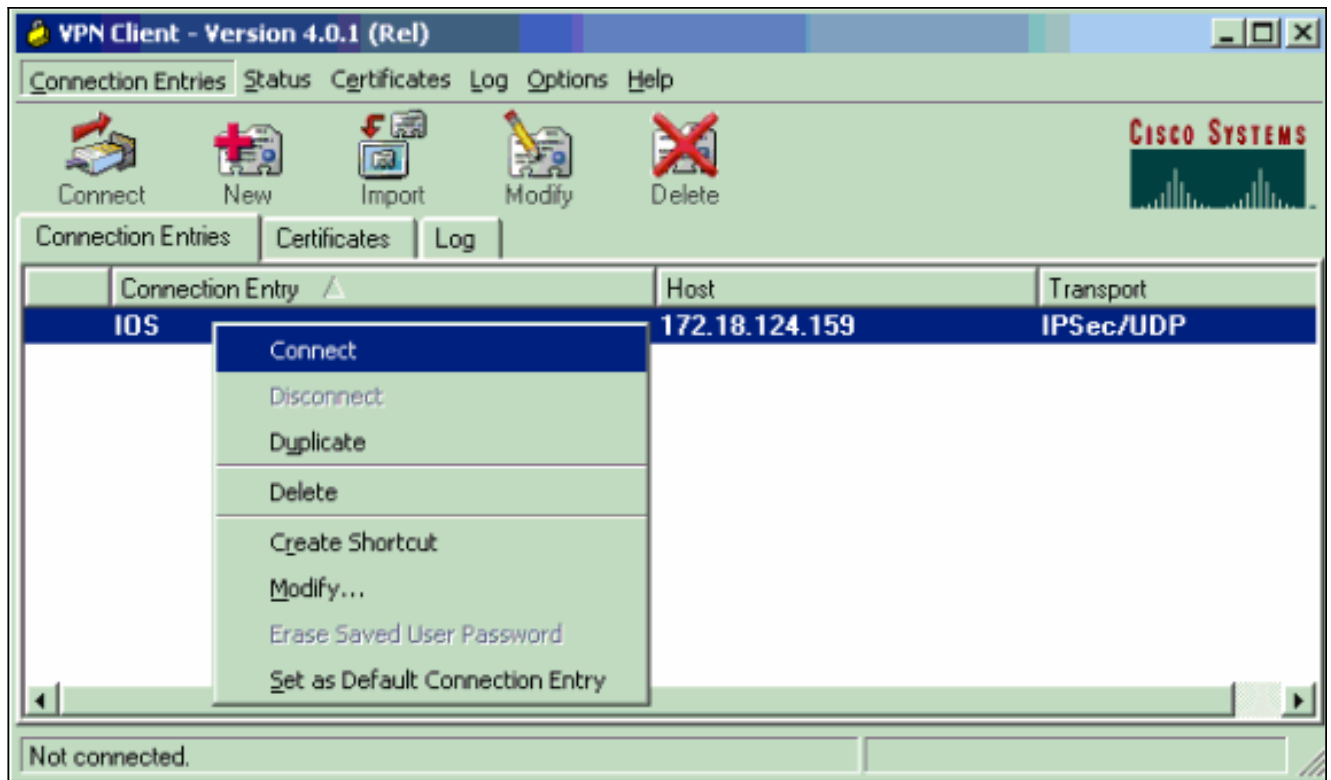
1. VPN Client を起動し、New をクリックして新しい接続を作成します。



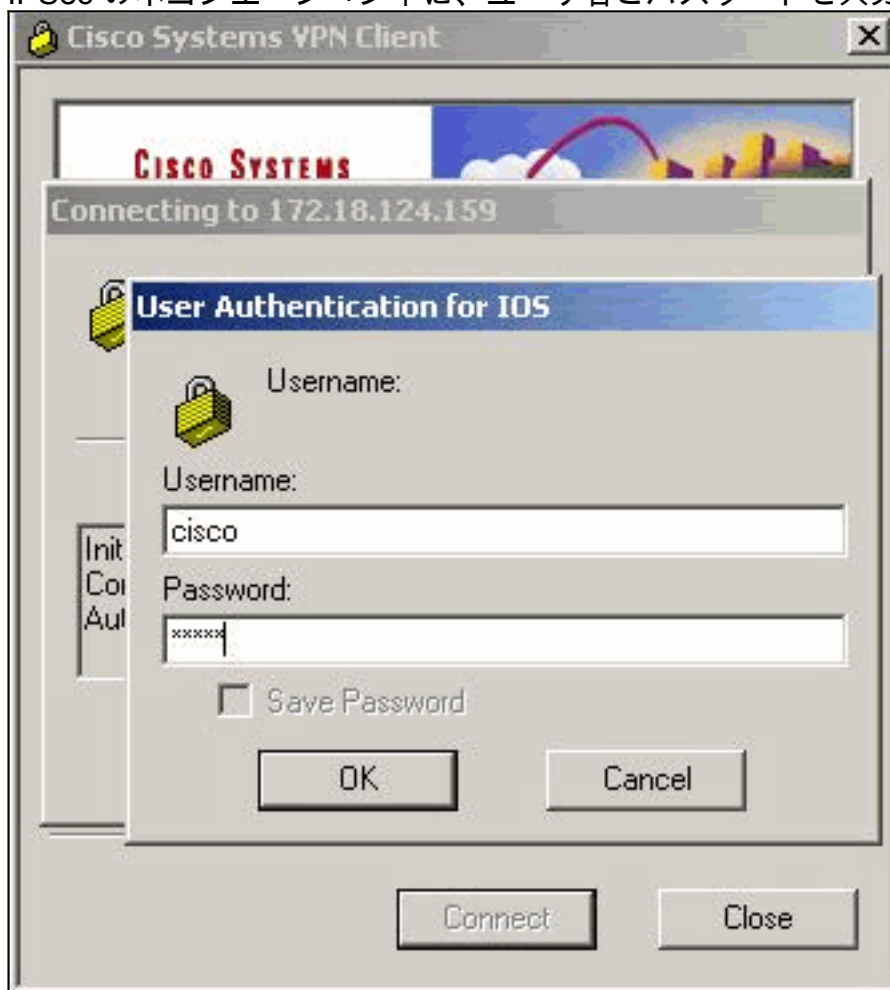
2. 必要な情報を入力し、終了したら Save をクリックします。



3. 新しく作成した接続エントリを右クリックし、Connect をクリックしてルータに接続します。



4. IPSec のネゴシエーション中に、ユーザ名とパスワードを入力するように求められます。



5. ウィンドウに「Negotiating security profiles」および「Your link is now secure」というメッセージが表示されます。

確認

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

。

一部の show コマンドは[アウトプット インタープリタ ツールによってサポートされています \(登録ユーザ専用\)](#)。このツールを使用することによって、show コマンド出力の分析結果を表示できます。

Cisco VPN 2611

```
vpn2611#show crypto isakmp sa
dst src state conn-id slot
172.18.124.159 172.18.124.199 QM_IDLE 5 0
!--- For the LAN-to-LAN tunnel peer. 172.18.124.159 64.102.55.142 QM_IDLE 6 0
!--- For the Cisco Unity Client tunnel peer. vpn2611#show crypto ipsec sa

interface: Ethernet0/0
Crypto map tag: clientmap, local addr. 172.18.124.159

protected vrf:
local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.10.20.0/255.255.255.0/0/0)
current_peer: 172.18.124.199:500
!--- For the LAN-to-LAN tunnel peer. PERMIT, flags={origin_is_acl,} #pkts encaps: 4, #pkts
encrypt: 4, #pkts digest 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4
#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.: 172.18.124.159, remote crypto endpt.:
172.18.124.199
path mtu 1500, media mtu 1500
current outbound spi: 892741BC

inbound esp sas:
spi: 0x7B7B2015(2071666709)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2000, flow_id: 1, crypto map: clientmap
sa timing: remaining key lifetime (k/sec): (4607999/1182)
IV size: 8 bytes
replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound ESP sas:
spi: 0x892741BC(2301051324)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2001, flow_id: 2, crypto map: clientmap
sa timing: remaining key lifetime (k/sec): (4607999/1182)
IV size: 8 bytes
replay detection support: Y

outbound ah sas:

outbound PCP sas:
```

protected vrf:
local ident (addr/mask/prot/port): (172.18.124.159/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (14.1.1.106/255.255.255.255/0/0)
current_peer: 64.102.55.142:500
!--- For the Cisco Unity Client tunnel peer. PERMIT, flags={} **#pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0**
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
#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.: 172.18.124.159, remote crypto endpt.:
64.102.55.142
path mtu 1500, media mtu 1500
current outbound spi: 81F39EFA

inbound ESP sas:
spi: 0xC4483102(3293065474)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2002, flow_id: 3, crypto map: clientmap
sa timing: remaining key lifetime (k/sec): (4608000/3484)
IV size: 8 bytes
replay detection support: Y

inbound ah sas:

inbound PCP sas:

outbound ESP sas:
spi: 0x81F39EFA(2180226810)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2003, flow_id: 4, crypto map: clientmap
sa timing: remaining key lifetime (k/sec): (4608000/3484)
IV size: 8 bytes
replay detection support: Y

outbound ah sas:

outbound PCP sas:

protected vrf:
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (14.1.1.106/255.255.255.255/0/0)
current_peer: 64.102.55.142:500
!--- For the Cisco Unity Client tunnel peer. PERMIT, flags={} **#pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4**
#pkts decaps: 20, #pkts decrypt: 20, #pkts verify 20
#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.: 172.18.124.159, remote crypto endpt.:
64.102.55.142
path mtu 1500, media mtu 1500
current outbound spi: B7F84138

inbound ESP sas:
spi: 0x5209917C(1376358780)
transform: esp-3des esp-md5-hmac ,

```
in use settings = {Tunnel, }
slot: 0, conn id: 2004, flow_id: 5, crypto map: clientmap
sa timing: remaining key lifetime (k/sec): (4607998/3474)
IV size: 8 bytes
replay detection support: Y
spi: 0xDE6C99C0(3731659200)
transform: esp-3des esp-md5-hmac ,
in use settings = {Tunnel, }
slot: 0, conn id: 2006, flow_id: 7, crypto map: clientmap
sa timing: remaining key lifetime (k/sec): (4607998/3493)
IV size: 8 bytes
replay detection support: Y
```

inbound ah sas:

inbound PCP sas:

```
outbound ESP sas:
spi: 0x58886878(1485334648)
transform: esp-3des esp-md5-hmac ,
in use settings = {Tunnel, }
slot: 0, conn id: 2005, flow_id: 6, crypto map: clientmap
sa timing: remaining key lifetime (k/sec): (4608000/3474)
IV size: 8 bytes
replay detection support: Y
spi: 0xB7F84138(3086500152)
transform: esp-3des esp-md5-hmac ,
in use settings = {Tunnel, }
slot: 0, conn id: 2007, flow_id: 8, crypto map: clientmap
sa timing: remaining key lifetime (k/sec): (4607999/3486)
IV size: 8 bytes
replay detection support: Y
```

outbound ah sas:

outbound PCP sas:

```
vpn2611#show crypto engine connection active
ID Interface IP-Address State Algorithm Encrypt Decrypt
5 Ethernet0/0 172.18.124.159 set HMAC_MD5+DES_56_CB 0 0
6 Ethernet0/0 172.18.124.159 set HMAC_SHA+3DES_56_C 0 0
2000 Ethernet0/0 172.18.124.159 set HMAC_MD5+3DES_56_C 0 4
2001 Ethernet0/0 172.18.124.159 set HMAC_MD5+3DES_56_C 4 0
2002 Ethernet0/0 172.18.124.159 set HMAC_MD5+3DES_56_C 0 0
2003 Ethernet0/0 172.18.124.159 set HMAC_MD5+3DES_56_C 0 0
2004 Ethernet0/0 172.18.124.159 set HMAC_MD5+3DES_56_C 0 9
2005 Ethernet0/0 172.18.124.159 set HMAC_MD5+3DES_56_C 0 0
2006 Ethernet0/0 172.18.124.159 set HMAC_MD5+3DES_56_C 0 79
2007 Ethernet0/0 172.18.124.159 set HMAC_MD5+3DES_56_C 4 0
vpn2611#
```

[Cisco VPN 3640](#)

```
vpn3640#show crypto isakmp sa
DST src state conn-id slot
172.18.124.159 172.18.124.199 QM_IDLE 4 0
!--- For the LAN-to-LAN tunnel peer. vpn3640#show crypto ipsec sa

interface: Ethernet0/0
```

Crypto map tag: mymap, local addr. 172.18.124.199

protected vrf:

local ident (addr/mask/prot/port): (10.10.20.0/255.255.255.0/0/0)

remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)

current_peer: 172.18.124.159:500

!--- For the LAN-to-LAN tunnel peer. PERMIT, flags={origin_is_acl,} #pkts encaps: 4, #pkts

encrypt: 4, #pkts digest 4

#pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. Failed: 0, #pkts decompress failed: 0

#send errors 11, #recv errors 0

local crypto endpt.: 172.18.124.199, remote crypto endpt.: 172.18.124.159

path mtu 1500, media mtu 1500

current outbound spi: 7B7B2015

inbound ESP sas:

spi: 0x892741BC(2301051324)

transform: esp-3des esp-md5-hmac ,

in use settings ={Tunnel, }

slot: 0, conn id: 940, flow_id: 1, crypto map: mymap

sa timing: remaining key lifetime (k/sec): (4607998/1237)

IV size: 8 bytes

replay detection support: Y

inbound ah sas:

inbound PCP sas:

outbound ESP sas:

spi: 0x7B7B2015(2071666709)

transform: esp-3des esp-md5-hmac ,

in use settings ={Tunnel, }

slot: 0, conn id: 941, flow_id: 2, crypto map: mymap

sa timing: remaining key lifetime (k/sec): (4607999/1237)

IV size: 8 bytes

replay detection support: Y

outbound ah sas:

outbound PCP sas:

vpn3640# show crypto engine connection active

ID Interface IP-Address State Algorithm Encrypt Decrypt

4

940 Ethernet0/0 172.18.124.199 set HMAC_MD5+3DES_56_C 0 4

941 Ethernet0/0 172.18.124.199 set HMAC_MD5+3DES_56_C 4 0

クリプト マップのシーケンス番号の確認

スタティックおよびダイナミックなピアが同じクリプト マップで設定されている場合、クリプト マップのエントリの順序は非常に重要です。ダイナミック暗証マップのエントリのシーケンス番号は、他のスタティック暗証マップのすべてのエントリよりも大きい必要があります。スタティック エントリにダイナミック エントリよりも大きな番号付けがされている場合、これらのピアで

の接続は失敗します。

スタティック エントリとダイナミック エントリが含まれるクリプト マップの、正しい番号付けの例を次に示します。ダイナミック エントリのシーケンス番号が最も大きく、また、ある程度の余裕を持たせてスタティック エントリを追加できるようにしています。

```
crypto dynamic-map dynmap 10
set transform-set myset
crypto map clientmap 1 ipsec-isakmp
set peer 172.18.124.199
set transform-set myset
match address 100
crypto map clientmap 10 ipsec-isakmp dynamic dynmap
```

トラブルシューティング

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情報を示します。

トラブルシューティングのためのコマンド

一部の show コマンドは [アウトプット インタープリタ ツールによってサポートされています \(登録ユーザ専用\)](#)。このツールを使用することによって、show コマンド出力の分析結果を表示できます。

注 : debug コマンドを発行する前に、[『debug コマンドの重要な情報』](#)を参照してください。

- debug crypto ipsec : IPsec イベントを表示します。このコマンドを no 形式で使用すると、デバッグ出力が無効になります。
- debug crypto isakmp : IKE イベントに関するメッセージを表示します。このコマンドを no 形式で使用すると、デバッグ出力が無効になります。
- debug crypto engine: Cisco IOS ソフトウェアが暗号化または復号化操作を実行する場合など、暗号化エンジンに関連する情報を表示します。

関連情報

- [IPSec ネゴシエーション/IKE プロトコルに関するサポート ページ](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)