# Microsoft Windows 2000 サーバとCiscoデバイス 間のIPSec 設定

### 内容

概要 はじめに 表記法 前提条件 <u>使用するコンポーネント</u> ネットワーク図 Microsoft Windows 2000 Server とシスコ デバイスを連携させるための設定 実行されるタスク 手順ごとの説明 Ciscoデバイスの設定 Cisco 3640 ルータの設定 PIX の設定 VPN 3000 コンセントレータの設定 VPN 5000 コンセントレータの設定 確認 トラブルシュート <u>トラブルシュー</u>ティングのためのコマンド 関連情報

### <u>概要</u>

このドキュメントでは、2 つのプライベート ネットワークに参加するための、事前共有キーを使 用した IPSec トンネルを構成する方法を示します。シスコ デバイス内部のプライベート ネット ワーク(192.168.I.X)内部および Microsoft 2000 Server 内部のプライベート ネットワーク (10.32.50.X)。シスコ デバイス内部と 2000 Server 内部からのインターネットへのトラフィッ ク(ここでは 172.18.124.X ネットワークで表します)は、この設定を開始する前から流れている ものと想定します。

Microsoft Windows 2000 Server 設定に関する詳細情報は、次の Microsoft ウェブ サイトにあります。<u>http://support.microsoft.com/support/kb/articles/Q252/7/35.ASP</u>

# <u>はじめに</u>

### <u>表記法</u>

ドキュメント表記の詳細は、『<u>シスコ テクニカル ティップスの表記法</u>』を参照してください。

このドキュメントに関しては個別の前提条件はありません。

### <u>使用するコンポーネント</u>

この構成は、次のソフトウェアとハードウェアのバージョンを使用して開発およびテストされて います。

- Microsoft Windows 2000 Server 5.00.2195
- Cisco 3640 ルータと Cisco IOS(R) Software リリース c3640-ik2o3s-mz.121-5.T.bin
- ・Cisco Secure PIX Firewall と PIX Software リリース 5.2.1
- Cisco VPN 3000 コンセントレータ と VPN 3000 コンセントレータ ソフトウェア バージョン 2.5.2.F
- Cisco VPN 5000 コンセントレータ と VPN 5000 コンセントレータ ソフトウェア バージョン 5.2.19

このマニュアルの情報は、特定のラボ環境に置かれた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。実稼動中のネットワークで作業をしている場合、実際にコマンドを使用する前に、その潜在 的な影響について理解しておく必要があります。

#### <u>ネットワーク図</u>

このドキュメントでは次の図に示すネットワーク構成を使用しています。



## <u>Microsoft Windows 2000 Server とシスコ デバイスを連携させる</u> ための設定

<u>実行されるタスク</u>



### <u>手順ごとの説明</u>

MicrosoftのWebサイトで設定の手順に従っ<u>た</u>、次の手順を使用して、設定がシスコデバイスで動作することを確認します。コメントと変更が、スクリーン キャプチャとともに示されています。

1. Microsoft Windows 2000 Server の [スタート] > [実行] > [secpol.msc] をクリックして、次の 画面で情報を検証します。Microsoft ウェブ サイトの手順を使用して 2000 サーバを設定し た後で、次のトンネル情報が表示されています。**注:例**のルールは「to\_cisco」と呼ばれま す。

🛃 Local Security Settings	
_ Action View   ← →   🗈 📧   🗙 📅 💀 😰 ] 🏦 🎰   🖺 🧕	
Tree Name A Description	Policy Assigned
Name       Description         Security Settings       Cient (Respond Only)       Communicate normally (uns         Compute Security Policies       Secure Server (Requir       For all IP traffic, always req         Public Key Policies       Server (Request Secu       For all IP traffic, always req         IP Security Policies on       Server (Request Secu       For all IP traffic, always req	No No Yes

2. このルールの例には、2つのフィルタが含まれています。Microsoft-CiscoおよびCisco-

to_ciso	co Properties			? ×
Rules	S General			
	Security rules fo	or communicating with oth	ner computers	
IP S	Security Rules:			
IP	PFilter List	Filter Action	Authentication	Tu
	Microsoft-Cisco	Permit	Preshared Key	17
	Cisco-Microsoft	Permit	Preshared Key	17
	<dynamic></dynamic>	Default Response	Preshared Key	Nc
•				F
	A <u>d</u> d <u>E</u> dit	<u>R</u> emove	🔽 Use Add <u>W</u> ize	ard
osoft		Close	ancel <u>App</u>	ly.

3. Cisco-Microsoft IP Security Ruleを選択し、**Edit**をクリックして、IPフィルタリストを表示 /追加/編集します。

Edit Rule Properties ? 🗙
Authentication Methods Tunnel Setting Connection Type IP Filter List Filter Action
The selected IP filter list specifies which network traffic will be secured with this rule.
IP Filter Lists:
Name Description
O All ICMP Traffic Matches all ICMP packets betw O All IP Traffic Matches all IP packets from this
Cisco-Microsoft Microsoft-Cisco
Add Edit Remove
OK Cancel Apply

4. ルールの[一般] > [詳細] タブには IKE ライフタイム(480 分 = 28800 秒)が表示されていま

to	o_cisco Properties ??
ſ	Rules General
Ì	
	Key Exchange Settings
	Master key Perfect Forward Secrecy
	Authenticate and generate a new key after every:
	480 minutes
	Authenticate and generate a new key after every:
	0 session(s)
	Protect identities with these security methods:
	Methods
	Internet Key Exchange (IKE) for Windows 2000
	Jointy developed by Microsoft and Cisco Systems, Inc.
	OK Cancel
ŀ	Advanced
_	
	OK Cancel Apply

5. ルールの [一般] > [詳細] > [方式] タブには IKE 暗号化方式(DES)、IKE ハッシング (SHA1)、および Diffie-Helman グループ(Low(1))が表示されています。



6. 各フィルタには、5 つのタブがあります。認証方式(IKE の事前共有キー

Rule Properties		? ×
IP Filter List Authentication Methods	   Tunnel Setting	Filter Action
The authentica between the co authentication r another comput	tion method specifies h omputers. Offer and acc methods when negotiat ter.	ow trust is established ept these ing security with
Authentication Method prefer	rence order:	
Method	Details	Add
Preshared Key	cisco123	Edit Remove
		Move up
		Move down
[	ОК Са	ancel Apply

	IP Filter List Filter Action
	Authentication Methods Tunnel Setting Connection Type
	This rule only applies to network traffic over connections of the selected type.
	C All network connections
	<ul> <li>Local area network (LAN)</li> </ul>
	C Remote access
_	
	OK Cancel Apply

Authentic	ation Methods   T IP Filter List	unnel Setting	Connection Type Filter Action
Silter Action	The selected filter act for secure network tra	ion specifies whe affic, and how it v	ether this rule negotiate: vill secure the traffic.
Name	18.	Description	
O IPSec	tunnel	·	
O Permit O Reque O Requi	st Security (Optional) e Security	Permit unsec Accepts unse Accepts unse	ured IP packets to ecured communicat ecured communicat
Add	Edit	Remove	🔲 Use Add Wizard
Auu			

ルタの動作] > [IPSec トンネル] > [編集] > [編集]を選択して、[カスタム]をクリックします。

Modify Security Method	
Security Method	
<ul> <li>High (ESP)</li> <li>Data will be encrypted, authentic and unmodified</li> </ul>	
<ul> <li>Medium (AH)</li> <li>Data will be authentic and unmodified, but will not be encrypted</li> <li>Custom (for expert users)</li> <li>Settings</li> </ul>	
OK Cancel Apply	

トランスフォーム] と [IPSec ライフタイム] をクリックします。

Custom Security Method Settings	? ×	
Specify the settings for this custom secur	ity method.	
Data and address integrity without en Integrity algorithm:	cryption (AH) :	
MD5 💌		
Data integrity and encryption (ESP): Integrity algorithm: MD5		
Encryption algorithm:		
Session Key Settings:		
Generate a new key every:	🔽 Generate a new key every	
100000 Kbytes	3600 seconds	
	OK Cancel	  Pフィルタリスト

暗号化する送信元および宛先ネットワーク:Cisco-Microsoftの場合

🛢 IP Filter l	list						?
<b>≣</b> <sup>/</sup>	An IP filter list is compo addresses and protocol	sed of multiple filte Is can be combine	rs. In this way multiple sub d into one IP filter.	nets, IP			
Name:				,			
Cisco-Micr	rosoft						
Description	κ						Add
			<u>^</u>				Edit
			<b>x</b>				Remove
Filters:			_				Use Add Wizard
Mirrored	Description	Protocol	Source Port	Destination Port	Source DNS Name	Source Address	Source Ma
Yes		ANY	ANY	ANY	<a ip="" specific="" sub<="" td=""><td>192.168.1.0</td><td>255.255.25</td></a>	192.168.1.0	255.255.25
•							Þ
						OK	Canad
						01	

\_

Microsoft-

Cisco:

.

IP Filter L	ist					?
	an IP filter list is con addresses and prote	nposed of multiple filte ocols can be combine	ers. In this way multiple su d into one IP filter.	bnets, IP		
Name:						
Microsoft-0	Lisco					
Description	c					Add
			*			Edit
			<b>v</b>			Remove
Filters:					<b>T</b>	Use Add Wizard
Mirrored	Description	Protocol	Source Port	Destination Port	Source DNS Name	Source Address
Yes		ANY	ANY	ANY	<a ip="" specific="" sub<="" td=""><td>10.32.50.0</td></a>	10.32.50.0
•						•
					OK	Cancel

トンネルの設定値:暗号化ピアCisco-Microsoftの場合

IP Filter List       Filter Action         Authentication Methods       Tunnel Setting       Connection Type	IP Filter List       Filter Action         Authentication Methods       Tunnel Setting       Connection Type         Image: Construction Methods       Total Setting       Connecting	IP Filter List       Filter Action         Authentication Methods       Tunnel Setting       Connection Type         Image: Construction Methods       Construction Methods       Construction Methods         Image: Construction Methods       Tunnel Setting       Connection Type         Image: Construction Methods       Tunnel Setting       Connection Type         Image: Construction Methods       Tunnel Setting       Connection Type         Image: Construction Methods       Tunnel Setting       Construction Type         Image: Construction Methods       Tunnel Setting       Constructio	Rule P	roperties			? ×
<ul> <li>The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the associated IP Filter List. It takes two rules to describe an IPSec Tunnel.</li> <li>This rule does not specify an IPSec tunnel.</li> <li>The tunnel endpoint is specified by this IP Address:</li> <li>172.18.124.157</li> </ul>	<ul> <li>The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the associated IP Filter List. It takes two rules to describe an IPSec Tunnel.</li> <li>This rule does not specify an IPSec tunnel.</li> <li>The tunnel endpoint is specified by this IP Address:</li> <li>172.18.124.157</li> </ul>	<ul> <li>The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the associated IP Filter List. It takes two rules to describe an IPSec Tunnel.</li> <li>This rule does not specify an IPSec tunnel.</li> <li>The tunnel endpoint is specified by this IP Address:</li> <li>172.18.124.157</li> </ul>	Authen	IP Filter List tication Methods	 Tunnel Setting	Filter Action	
<ul> <li>This rule does not specify an IPSec tunnel.</li> <li>The tunnel endpoint is specified by this IP Address:</li> <li>172.18.124.157</li> </ul>	<ul> <li>This rule does not specify an IPSec tunnel.</li> <li>The tunnel endpoint is specified by this IP Address:</li> <li>172.18.124.157</li> </ul>	<ul> <li>This rule does not specify an IPSec tunnel.</li> <li>The tunnel endpoint is specified by this IP Address:</li> <li>172.18.124.157</li> </ul>		The tunnel endpo IP traffic destinat List. It takes two	oint is the tunneling c ion, as specified by th rules to describe an II	omputer closest to th ne associated IP Filte PSec Tunnel.	e r
172.18.124.157	172.18.124.157	172.18.124.157	O This ⊙ The∣	rule does not specify a :unnel endpoint is spe	an IPSec tunnel. cified by this IP Addre	155:	
			1	72.18.124.1	157		
OK Cancel Apply	OK Cancel Apply				ок С	ancel Appl	U .

E	dit Rule Properties		? ×
	IP Filter List Authentication Methods	Tunnel Setting	Filter Action
	The tunnel end IP traffic destina List. It takes two	point is the tunneling co ation, as specified by the prules to describe an IF	omputer closest to the e associated IP Filter PSec Tunnel.
	<ul> <li>This rule does not specify</li> <li>The tunnel endpoint is sp</li> <li>172.18.124.</li> </ul>	an IPSec tunnel. ecified by this IP Addre: <b>35</b>	\$\$:
isco:	[	OK Ca	ancel Apply

# <u>Ciscoデバイスの設定</u>

次の例に示すように、Ciscoルータ、PIX、およびVPNコンセントレータを設定します。

- <u>Cisco 3640 ルータ</u>
- <u>PIX</u>
- <u>VPN 3000 コンセントレータ</u>
- <u>VPN 5000 コンセントレータ</u>

### <u>Cisco 3640 ルータの設定</u>

#### Cisco 3640 ルータ

```
Current configuration : 1840 bytes
!
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
```

```
service timestamps log uptime
no service password-encryption
hostname moss
logging rate-limit console 10 except errors
ip subnet-zero
no ip finger
1
ip audit notify log
ip audit po max-events 100
crypto isakmp policy 1
!--- The following are IOS defaults so they do not
appear: !--- IKE encryption method encryption des !---
IKE hashing hash sha !--- Diffie-Hellman group group 1
!--- Authentication method authentication pre-share
!--- IKE lifetime lifetime 28800
!--- encryption peer crypto isakmp key cisco123 address
172.18.124.157
!--- The following is the IOS default so it does not
appear: !--- IPSec lifetime crypto ipsec security-
association lifetime seconds 3600 ! !--- IPSec
transforms crypto ipsec transform-set rtpset esp-des
esp-md5-hmac
crypto map rtp 1 ipsec-isakmp
!--- Encryption peer set peer 172.18.124.157
set transform-set rtpset
!--- Source/Destination networks defined match address
115
1
call rsvp-sync
!
interface Ethernet0/0
ip address 192.168.1.1 255.255.255.0
ip nat inside
half-duplex
1
interface Ethernet0/1
ip address 172.18.124.35 255.255.255.240
ip nat outside
half-duplex
crypto map rtp
1
ip nat pool INTERNET 172.18.124.35 172.18.124.35 netmask
255.255.255.240
ip nat inside source route-map nonat pool INTERNET
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.124.36
no ip http server
1
access-list 101 deny ip 192.168.1.0 0.0.0.255 10.32.50.0
0.0.0.255
access-list 101 permit ip 192.168.1.0 0.0.0.255 any
!--- Source/Destination networks defined access-list 115
permit ip 192.168.1.0 0.0.0.255 10.32.50.0 0.0.0.255
access-list 115 deny ip 192.168.1.0 0.0.0.255 any
route-map nonat permit 10
match ip address 101
```

### <u>PIX の設定</u>

PIX			
PIX Version 5.2(1)			
nameif ethernet0 outside securitv0			
nameif ethernet1 inside security100			
enable password 8Rv2YiTvt7RRXII24 encrypted			
passwd 2KEOnbNIdI 2KVOU encrypted			
hostname pixfirewall			
fixup protocol ftp 21			
fixup protocol http 80			
fixup protocol $h323$ 1720			
fixup protocol rsh 514			
fixup protocol smtp 25			
fixup protocol salpot 1521			
fixup protocol sin 5060			
names			
names			
Source/Descination networks defined access-fist fis			
permit 1p 192.108.1.0 255.255.255.0 10.32.50.0			
access-list 115 denv ip 192.168.1.0 255.255.255.0 anv			
pager lines 24			
logging on			
no logging timestamp			
no logging standby			
no logging console			
no logging monitor			
no logging huffered			
no logging tran			
no logging bistory			
ho logging history			
logging facility 20			
interface athemat() auto			
interface ethernett 10keest			
Interface etherneti lubaset			
mtu outside 1500			
mtu inside 1500			
1p address outside 172.18.124.35 255.255.255.240			
1p address inside 192.168.1.1 255.255.255.0			
ip audit info action alarm			
ip audit attack action alarm			
no failover			
failover timeout 0:00:00			
failover poll 15			
failover ip address outside 0.0.0.0			
failover ip address inside 0.0.0.0			
arp timeout 14400			
<pre>! Except Source/Destination from Network Address</pre>			
Translation (NAT): nat (inside) 0 access-list 115			
route outside 0.0.0.0 0.0.0.0 172.18.124.36 1			
timeout xlate 3:00:00			
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc			
0:10:00 h323 0:05:00			

sip 0:30:00 sip\_media 0:02:00 timeout uauth 0:05:00 absolute aaa-server TACACS+ protocol tacacs+ aaa-server RADIUS protocol radius no snmp-server location no snmp-server contact snmp-server community public no snmp-server enable traps floodguard enable sysopt connection permit-ipsec no sysopt route dnat !--- IPSec transforms crypto ipsec transform-set myset esp-des esp-md5-hmac !--- IPSec lifetime crypto ipsec security-association lifetime seconds 3600 crypto map rtpmap 10 ipsec-isakmp !--- Source/Destination networks crypto map rtpmap 10 match address 115 !--- Encryption peer crypto map rtpmap 10 set peer 172.18.124.157 crypto map rtpmap 10 set transform-set myset crypto map rtpmap interface outside isakmp enable outside !--- Encryption peer isakmp key \*\*\*\*\*\*\* address 172.18.124.157 netmask 255.255.255.240 isakmp identity address !--- Authentication method isakmp policy 10 authentication pre-share !--- IKE encryption method isakmp policy 10 encryption des !--- IKE hashing isakmp policy 10 hash sha !--- Diffie-Hellman group isakmp policy 10 group 1 !--- IKE lifetime isakmp policy 10 lifetime 28800 telnet timeout 5 ssh timeout 5 terminal width 80 Cryptochecksum:c237ed11307abea7b530bbd0c2b2ec08 : end

#### <u>VPN 3000 コンセントレータの設定</u>

必要に応じてVPNコンセントレータを設定するには、次に示すメニューオプションとパラメータ を使用します。

```
    (設定) > [システム] > [トンネリングプロトコル] > [IPSec] > [IKE 提案] > [提案の追加]:

Proposal Name = DES-SHA

    /--- Authentication method Authentication Mode = Preshared Keys /--- IKE hashing

Authentication Algorithm = SHA/HMAC-160 /--- IKE encryption method Encryption Algorithm =

DES-56 /--- Diffie-Hellman group Diffie Hellman Group = Group 1 (768-bits) Lifetime

Measurement = Time Date Lifetime = 10000 /--- IKE lifetime Time Lifetime = 28800
    LAN-to-LANトンネルを定義するには、Configuration > System > Tunneling Protocols > IPSec

LAN-to-LANの順に選択します。

Name = to_2000
```

```
Interface = Ethernet 2 (Public) 172.18.124.35/28

!--- Encryption peer Peer = 172.18.124.157 !--- Authentication method Digital Certs = none

(Use Pre-shared Keys) Pre-shared key = cisco123 !--- IPSec transforms Authentication =

ESP/MD5/HMAC-128 Encryption = DES-56 !--- Use the IKE proposal IKE Proposal = DES-SHA

Autodiscovery = off !--- Source network defined Local Network Network List = Use IP

Address/Wildcard-mask below IP Address 192.168.1.0 Wildcard Mask = 0.0.0.255 !---

Destination network defined Remote Network Network List = Use IP Address/Wildcard-mask below

IP Address 10.32.50.0 Wildcard Mask 0.0.0.255
```

#### セキュリティアソシエーションを変更するには、[Configuration] > [Policy Management] > [Traffic Management] > [Security Associations] > [Modify]を選択します。

```
SA Name = L2L-to_2000
Inheritance = From Rule
IPSec Parameters
/--- IPSec transforms Authentication Algorithm = ESP/MD5/HMAC-128 Encryption Algorithm =
DES-56 Encapsulation Mode = Tunnel PFS = Disabled Lifetime Measurement = Time Data Lifetime
= 10000 /--- IPSec lifetime Time Lifetime = 3600 Ike Parameters /--- Encryption peer IKE
Peer = 172.18.124.157 Negotiation Mode = Main /--- Authentication method Digital Certificate
= None (Use Preshared Keys) /--- Use the IKE proposal IKE Proposal DES-SHA
```

#### <u>VPN 5000 コンセントレータの設定</u>

# VPN 5000 コンセントレータ

```
[ IP Ethernet 1:0 ]
Mode = Routed
SubnetMask = 255.255.255.240
IPAddress = 172.18.124.35
[ General ]
IPSecGateway = 172.18.124.36
DeviceName = "cisco"
EthernetAddress = 00:00:a5:f0:c8:00
DeviceType = VPN 5002/8 Concentrator
ConfiguredOn = Timeserver not configured
ConfiguredFrom = Command Line, from Console
[ IP Ethernet 0:0 ]
Mode = Routed
SubnetMask = 255.255.255.0
IPAddress = 192.168.1.1
[ Tunnel Partner VPN 1 ]
!--- Encryption peer Partner = 172.18.124.157 !---
IPSec lifetime KeyLifeSecs = 3600 BindTo = "ethernet
1:0" !--- Authentication method SharedKey = "cisco123"
KeyManage = Auto !--- IPSec transforms Transform =
esp(md5,des) Mode = Main !--- Destination network
defined Peer = "10.32.50.0/24" !--- Source network
defined LocalAccess = "192.168.1.0/24" [ IP Static ]
10.32.50.0 255.255.255.0 VPN 1 1 [ IP VPN 1 ] Mode =
Routed Numbered = Off [ IKE Policy ] !--- IKE hashing,
encryption, Diffie-Hellman group Protection = SHA_DES_G1
Configuration size is 1088 out of 65500 bytes.
```

## <u>確認</u>

現在、この設定に使用できる確認手順はありません。

# <u>トラブルシュート</u>

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提供します。

### <u>トラブルシューティングのためのコマンド</u>

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

#### <u>Cisco 3640 ルータ</u>

- ・debug crypto engine :暗号化と暗号解除を実行する crypto エンジンに関するデバッグ メッ セージを表示します。
- ・debug crypto isakmp :IKE イベントに関するメッセージを表示します。
- debug crypto ipsec : IPSec イベントを表示します。
- show crypto isakmp sa: ピアの現在の IKE セキュリティ アソシエーション(SA) すべてを 表示します。
- show crypto ipsec sa :現在の SA が使用する設定を表示します。
- ・clear crypto isakmp :(設定モードから)すべてのアクティブな IKE 接続をクリアーします 。
- clear crypto sa :(設定モードから)すべての IPSec SAを削除します。

#### <u>PIX</u>

- ・debug crypto ipsec:IPSec ネゴシエーションのフェーズ 2 を表示します。
- debug crypto isakmp フェーズ1の Internet Security Association and Key Management Protocol (ISAKMP) ネゴシエーションを表示します。
- debug crypto engine:暗号化されたトラフィックを表示します。
- show crypto ipsec sa フェーズ2のセキュリティ アソシエーションを表示します。
- show crypto isakmp sa フェーズ1のセキュリティ結合を表示します。
- clear crypto isakmp :(設定モードから)Internet Key Exchange(IKE) SA をクリアーします。
- clear crypto ipsec sa :(設定モードから)IPSec SA を削除します。

#### <u>VPN 3000 コンセントレータ</u>

● VPN 3000 コンセントレータのデバッグを開始するために、[設定] > [システム] > [イベント] > [クラス] > [修正] を選択します(ログ重大度 =1-13、コンソール重大度 =1-3):IKE、

IKEDBG、IKEDECODE、IPSEC、IPSECDBG、IPSECDECODE

- イベント ログをクリアーまたは取得するには、[モニタリング] > [イベント ログ]を選択します。
- LAN-to-LAN トンネル トラフィックは[モニタリング] > [セッション]でモニタできます。
- トンネルをクリアーするには、[管理] > [セッションの管理] > [LAN-to-LAN セッション] > [ア クション・ログアウト]を選択します。

<u>VPN 5000 コンセントレータ</u>

• vpn trace dump all :すべての一致する VPN 接続の情報を表示します。時間、VPN 番号、ピアの実際の IP アドレス、どのスクリプトが実行されているかの情報、そしてエラーの場合は

エラーが発生したソフトウェア コードのルーチンと回線番号が表示されます。

- show vpn statistics:ユーザやパートナーの次の情報を表示します。(モジュラ モデルでは、ディスプレイには各モジュール スロットのセクションが含まれます)。 Current Active:現在アクティブな接続です。In Negot:現在ネゴシエート中の接続です。High Water:最後のリブート以降のアクティブな同時接続の最高数です。Running Total:最後のリブート以降の成功した接続の合計数です。Tunnel Starts:トンネル開始の数です。Tunnel OK:エラーのないトンネルの数です。Tunnel Error:エラーが発生したトンネルの数です。
- show vpn statistics verbose : ISAKMP ネゴシエーション統計情報と、さらに多数のアクティブ接続の統計情報を表示します。

# 関連情報

- Cisco VPN 5000 シリーズ コンセントレータの販売終了のお知らせ
- IPSec ネットワーク セキュリティの設定
- Internet Key Exchange セキュリティ プロトコルの設定
- <u>テクニカルサポート Cisco Systems</u>