Checkpoint 4.1 Firewall に対する IPSec トンネ ル - Cisco VPN 5000 コンセントレータの設定

内容

概要 前提条件 要件 <u>使用するコンポーネント</u> 表記法 設定 ネットワーク図 設定 **Checkpoint 4.1 Firewall** 確認 トラブルシュート VPN 5000 コンセントレータのトラブルシューティング コマンド <u>ネットワー</u>ク集約 Checkpoint 4.1 Firewall のデバッグ debug 出力例 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について説明します。これにより、Cisco VPN 5000 コンセントレータ(192.168.1.x)内部のプライベート ネットワークが、Checkpoint 4.1 Firewall(10.32.50.x)内部のプライベート ネットワークに参加します。 ここでは、この設定を始める前に、VPN コンセントレータ内部および Checkpoint 内部からインターネットへのトラフィック(ここでは 172.18.124.X と表現しています)が流れていることを前提としています。

前提条件

<u>要件</u>

このドキュメントに特有の要件はありません。

<u>使用するコンポーネント</u>

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 VPN 5000 コンセントレータ
- Cisco VPN 5000 コンセントレータ ソフトウェア バージョン 5.2.19.0001
- Checkpoint 4.1 Firewall

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。

<u>表記法</u>

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。

<u>設定</u>

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供して います。

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、<u>Command Lookup</u> <u>Tool(登録</u>ユーザ専用)を使用してください。

<u>ネットワーク図</u>

このドキュメントでは、次のネットワーク セットアップを使用します。



<u>設定</u>

このドキュメントでは次の設定を使用します。

Cisco VPN 5000 コンセントレータ		
[IP Ethernet 0:0]		
Mode	= Routed	
SubnetMask	= 255.255.255.0	
IPAddress	= 192.168.1.1	
[General]	- 00.00.25.00.08.00	
Dowigo	= VPN 5002/8 Concentrator	
Configuradon	- Win 5002/8 concentrator	
Configuredon	- Command Line from Concole	
	- Unicate and sint "	
DeviceName	= 172 19 124 24	
IPSecGaleway	= 172.18.124.34	
[IKE Policy]		
Protection	= SHA_DES_G2	
[Tunnel Partner VPN 1]		
KevLifeSecs	= 28800	
	= "192 168 1 0/24"	
Peer	= "10_32_50_0/24"	
BindTo	= "ethernet 1.0"	
SharedKey	= "ciscorules"	
KeyManage		
Transform	= esp(sha des)	
Partner	$= 172 \ 18 \ 124 \ 157$	
Mode	= 1,2.10.124.13,	
noue		
[IP VPN 1]		
Numbered	= Off	
Mode	= Routed	
[IP Ethernet 1:0]		
IPAddress	= 172.18.124.35	
SubnetMask	= 255,255,255,240	
Mode	= Routed	
[IP Static]		
10.32.50.0 255.255.255.0 VPN 1 1		
Configuration size is 1131 out of 65500 bytes.		

Checkpoint 4.1 Firewall

Checkpoint 4.1 Firewall を設定するには、次の手順を実行します。

1. [Properties] > [Encryption] を選択し、Checkpoint IPsec ライフタイムを VPN コンセントレ ータ コマンドの KeyLifeSecs = 28800 と一致するように設定します。注:チェックポイン トインターネットキーエクスチェンジ(IKE)ライフタイムはデフォルトのままにします。

Properties Setup	×
High Availability IP Pool NAT Access Security Policy Traffic Control Services Lo Authentication SYNDefender LDAP E	Lists Desktop Security og and Alert Security Servers Encryption ConnectControl
SKIP Enable Exportable SKIP Change SKIP Session Key :	Manual IPSEC SPI allocation range (hex):
Every 120 Seconds (0 for infinity) or Every 10485760 Butes (0 for infinity)	Erom 100
IKE Renegotiate I <u>K</u> E Security Associations every	440 minutes
Renegotiate I <u>P</u> SEC Security Associations every 28	3800 seconds
OK Cancel	Help

2. [Manage] > [Network objects] > [New](または [Edit])> [Network] の順に選択し、 Checkpoint の背後にある内部(「cpinside」)ネットワークのオブジェクトを設定します。 これは、VPN コンセントレータ コマンドの Peer = "10.32.50.0/24" と一致している必要が

etwork Properties	2
General NAT	
<u>N</u> ame: <mark>cpinside</mark>	
IP Address: 10.32.50.0	<u>G</u> et address
Net <u>M</u> ask: 255.255.255	.0
<u>C</u> omment:	Color:
Location: <u>Internal</u> <u>External</u>	Broadcast:
	1
OK	Cancel Help

3. [Manage] > [Network objects] > [Edit] の順に選択し、VPN コンセントレータが Partner = <ip>コマンドで指し示しているゲートウェイ(「RTPCPVPN」Checkpoint)エンドポイントのオブジェクトを編集します。[Location] の [Internal] を選択します。[Type] の [Gateway]を選択します。[Modules Installed] の下で、[VPN-1 & FireWall-1] と [Management Station]

あります

Workstation Properties	×
General Interfaces SNMP N	AT Certificates VPN Authe
Name: RTPCPVPN	
IP Address: 172.18.124.157	Get address
Comments Firewalled gatew	au to internet
<u>Commenc</u>	
	C Heat C Cateway
• Internal • External	
Modules Installed	
VPN-1 & <u>F</u> ireWall-1	Version: 4.1 💌 Get
FloodGate-1	Version: 4.1
Compre <u>s</u> sion	Version: 4.1
Management Station	Color:
	1
OK	Cancel Help

をオンにします。

4. [Manage] > [Network objects] > [New](または [Edit])> [Network] の順に選択し、VPN コン セントレータの背後にある外部(「inside_cisco」)ネットワークのオブジェクトを設定し ます。これは、VPN コンセントレータ コマンドの LocalAccess = <192.168.1.0/24> と一致 している必要があります。

Network Properties	×
General NAT	
<u>Name:</u> inside_cisco	
IP Address: 192.168.1.0	<u>G</u> et address
Net <u>M</u> ask: 255.255.255.0	
Comment:	Color: 🗾 💌
Location: ○ <u>I</u> nternal ⊙ <u>E</u> xternal	Broadcast: <u>A</u> llowed <u>D</u> isallowed
OK Ca	incel Help

5. [Manage] > [Network objects] > [New] > [Workstation] の順に選択し、外部(「 cisco_endpoint」)VPN コンセントレータ ゲートウェイのオブジェクトを追加します。これ は、Checkpoint への接続を持つ VPN コンセントレータの「外部」インターフェイスです (このドキュメントでは、172.18.124.35 は **IPAddress = <ip> コマンドの IP アドレス)。** [Location] の [External] を選択します。[Type] の [Gateway] を選択します。注: VPN-1/FireWall-1はチェックしないでください。

General Interfaces SNMP NAT VPN Name: Cisco_endpoint IP Address: 172.18.124.35 Get address Comment:	Workstation Properties
Name: cisco_endpoint IP Address: 172.18.124.35 Comment:	General Interfaces SNMP NAT VPN
IP Address: 172.18.124.35 Get address Comment:	Name: cisco endpoint
In gouress. Internet Comment: Type: O Internal O External Host O Gateway Modules Installed Image: Compression VPN-1 & FireWall-1 Version: Image: FloodGate-1 Version: Image: Compression Version: Image: Management Station Color:	IR Address: 172 18 124 35 Get address
Location: Type: ○ Internal ○ External ○ Host ○ Gateway Modules Installed ○ YPN-1 & FireWall-1 Version: 4.1 ♥ Get ○ FloodGate-1 Version: 4.1 ♥ Get ○ Compression Version: 4.1 ♥ Imagement Station ○ Management Station Color: Imagement Station	
○ Internal ○ External ○ Host ○ Gateway Modules Installed ○ VPN-1 & FireWall-1 Version: 4.1 ♥ ○ FloodGate-1 Version: 4.1 ♥ ○ Compression Version: 4.1 ♥ ○ Management Station Color:	Loomment:
Modules Installed VPN-1 & FireWall-1 Version: 4.1 FloodGate-1 Version: 4.1 Compregsion Version: 4.1 Management Station Color:	O Internal ⊙ External O Host ⊙ Gateway
□ VPN-1 & FireWall-1 Version: 4.1 ✓ □ FloodGate-1 Version: 4.1 ✓ □ Compression Version: 4.1 ✓ □ Management Station Color: ✓ ✓	Modules Installed
□ FloodGate-1 Version: 4.1 ▼ □ Compregsion Version: 4.1 ▼ □ Management Station Color: □ ▼	□ VPN-1 & <u>F</u> ireWall-1 Version: 4.1 <u>Get</u>
□ Compression Version: 4.1 ▼ □ Management Station Color: □ ▼	☐ FloodGate-1 Version: 4.1 ▼
☐ <u>M</u> anagement Station Co <u>l</u> or: ☐ ☐	Compression Version: 4.1
	□ <u>M</u> anagement Station Color: ▼
OK Cancel Help	

6. [Manage] > [Network objects] > [Edit] の順に選択し、Checkpoint ゲートウェイ エンドポイン ト(「RTPCPVPN」という名前)の [VPN] タブを編集します。[Domain] の下で、[Other] を 選択してから、Checkpoint ネットワークの内側(「cpinside」という名前)をドロップダウ ンリストから選択します。[Encryption schemes defined] の下で、[IKE] を選択してから [Edit] をクリックします。

Workstation Properties	×
General Interfaces SNMP NAT	Certificates VPN Authe
Domain: © Disabled © Valid Addresses(of Interfaces) © Other: Exportable for SecuRemote	Encryption <u>s</u> chemes defined:
Traffic Control Logging	ng
OK Car	ncel Help

7. VPN コンセントレータ コマンドの SHA_DES_G2 と一致するように IKE プロパティを [DES] 暗号化と [SHA1] ハッシュに変更します。注: 「G2」はDiffie-Hellmanグループ1また は2を指します。テストでは、Checkpointが「G2」または「G1」を受け入れることが検出さ れました。次の設定を変更します。[Aggressive Mode] をオフにします。[Supports Subnets] をオンにします。[Authentication Method] の [Pre-Shared Secret] をオンにします。

General Interfaces SNMP NAT Cer	tificates VPN Authe
KE Properties	×
General	
– Key <u>N</u> egotiation Encryption Method	d(s): – – <u>H</u> ash Method: –
DES DES	□ MD <u>5</u>
□ CAST □ 3DES	SHA1
- <u>A</u> uthentication Method:	
Pre-Shared Secret	Edit <u>S</u> ecrets
Public <u>K</u> ey Signatures	<u>C</u> onfigure
Supports Aggresive <u>M</u> ode 🔽	Supports Su <u>b</u> nets
OK Cancel	Help

8. [Edit Secrets] をクリックし、事前共有キーを VPN コンセントレータ コマンドの SharedKey = <key> と一致するように設定します。

Workstation Properties
General Interfaces SNMP NAT Certificates VPN Authe
IKE Properties 🔀 🔀
General
Shared Secret 🔀
Shared Secrets List:
Peer Name Shared Secret
cisco_endpoint **** <u>E</u> dit
Bemove
OK Cancel
OK Cancel Help
OK Cancel Help

9. [Manage] > [Network objects] > [Edit] の順に選択し、「cisco_endpoint」の [VPN] タブを編 集します。[Domain] の下で、[Other] を選択してから、VPN コンセントレータ ネットワーク の内側(「inside_cisco」という名前)を選択します。 [Encryption schemes defined] の下で 、[IKE] を選択してから [Edit] をクリックします。

Workstation Properties	×
General Interfaces SNMP NAT	VPN
2	
Domain:	Encryption schemes defined:
C <u>D</u> isabled	Manual IPSEC
○ <u>V</u> alid Addresses(of Interfaces)	🗹 🗽 KE
Other:	🗆 🖬 SKIP
💂 inside_cisco 🔻	
Euportable for SecuBerrote	E dù
	<u> </u>
Traffic Control Logging	
🔽 Turn on Traffic Control Loggi	ng
OK Ca	ncel Help

10. VPN コンセントレータ コマンドの SHA_DES_G2 と一致するように IKE プロパティを [DES] 暗号化と [SHA1] ハッシュに変更します。注: 「G2」はDiffie-Hellmanグループ1ま たは2を指します。テストでは、Checkpointが「G2」または「G1」を受け入れていること が判明しました。次の設定を変更します。[Aggressive Mode] をオフにします。[Supports Subnets] をオンにします。[Authentication Method] の [Pre-Shared Secret] をオンにします

General Interfaces SNMP NAT Certificates VPN Authe
KE Properties 🔀
General
Key <u>N</u> egotiation Encryption Method(s): <u>H</u> ash Method:
I I I I I I I I I I I I I I I I I I I
□ 🖾 3DES 🔽 SHA <u>1</u>
Authentication Method:
✓ Pre-Shared Secret Edit Secrets
Public Key Signatures Configure
Supports Aggresive Mode Supports Subnets
OK Cancel Help

11. [Edit Secrets] をクリックし、事前共有キーを VPN コンセントレータ コマンドの SharedKey = <key> と一致するように設定します。

o

IKE Properties	×
General	
Shared Secret X	1
- Shared Secrets List:	L
Peer Name Shared Secret	
RTPCPVPN **** <u>E</u> dit	
Bemove	
OK Cancel	
	۲,
OK Cancel Help	

12. [Policy Editor] ウィンドウで、Source と Destination の両方に「inside_cisco」と「 cpinside」(双方向)を設定したルールを挿入します。 Service=Any、Action=Encrypt、お よび Track=Long を設定します。

1	RTPO	PVPN - Check P	oint Policy Editor					_ 🗆 🗵
ł	Eile <u>E</u> di	t <u>V</u> iew <u>M</u> anage	Policy Window <u>H</u>	elp				
	- 5	🖪 🔍 👗 🖻	E 💁 🕉 🕉	🖳 🐬 🖉	ا 🕾 🖄	* * •	T. 🔫 🖝	🖶 👺 🐺 🚯
	😫 Secu	urity Policy - Standard	🖥 🖶 Address Trans	slation - Standa	rd 🛛 😿 Bandw	idth Policy - S	tandard	
	No.	Source	Destination	Servio	e A	ction	Track	In
1	1	💂 inside_cisco 💂 cpinside	cpinside	Any	R	Encrypt	Long	
ļ	•							•
F	or Help,	press F1			RTPCPVPN	Rea	d/Write	

13. [Action] 見出しの下で、緑の [Encrypt] アイコンをクリックし、[Edit properties] を選択して 暗号化ポリシーを設定します。

rity Policy - Standard	Address Translation ·	Standard 报 Band	width Policy - Standard	- 0
∼ FVV1 Host	∼ Ldap-Servers	10 Idap	accept	
∼ FVV1 Host	∼ Logical-Servers	∼ load_agent	accept	1
nside_cisco	💂 cpinside 💂 inside_cisco	Any	dit properties	hg .
		icmp dest-unreach	Edit Encryption	
		icmp echo-request	accept	am í
		icmp info-reply	drop	
Any	Any	icmp mask-reply	🚺 🕒 reject	
•				Þ

14. [IKE] を選択してから [Edit] をクリックします。

Encryption Properties	×
General	
Encryption schemes defined:	
Edit	
OK Cancel Help	

15. [IKE Properties] ウィンドウで、これらのプロパティを VPN コンセントレータ コマンドの **Transform = esp(sha,des) と一致するように変更します。**[Transform] の [Encryption + Data Integrity (ESP)] を選択します。 [Encryption Algorithm] は [DES] に、[Data Integrity] は [SHA1] に、そして [Allowed Peer Gateway] は外部 VPN コンセントレータ ゲートウェイ (「cisco_endpoint」という名前)に、それぞれなります。 [OK] をクリックします。

IKE Properties	×
General	
- Transform:	
Encryption + Data Integrity (ESP)	
C Data Integrity Only (AH)	
Encryption Algorithm: DES	
Data Integrity SHA1	
Allowed Peer Gateway:	
Use Perfect Forward Secrecy	
OK Cancel Help	

16. Checkpoint の設定後、[Checkpoint] メニューで [Policy] > [Install] を選択し、変更内容を有 効にします。

<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>

VPN 5000 コンセントレータのトラブルシューティング コマンド

<u>アウトプット インタープリタ ツール(登録ユーザ専用)(OIT)は、特定の show コマンドをサ</u> <u>ポートします。</u>OIT を使用して、show コマンドの出力の分析を表示します。

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。

- 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 system log buffer : 内部ログ バッファの内容を表示します。
- 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。「<u>デバッグのサンプル出力」を参照してください)。</u>Current ActiveIn NegotHigh WaterRunning TotalTunnel OKTunnel StartsTunnel Error

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。

<u>ネットワーク集約</u>

暗号化ドメイン内の Checkpoint で複数の隣接する内部ネットワークが設定されている場合、この デバイスによってそれらのネットワークが特定のトラフィックに関して自動的に集約されること があります。VPN コンセントレータが適合するように設定されていない場合、このトンネルに障 害が発生する可能性があります。たとえば、10.0.0.0 /24 と 10.0.1.0 /24 の内部ネットワークがト ンネルに含まれるように設定されている場合、それらが 10.0.0.0 /23 に集約される可能性があり ます。

Checkpoint 4.1 Firewall のデバッグ

このデバッグは Microsoft Windows NT がインストールされている場合のものです。トラッキング は [Policy Editor] ウィンドウで Long <u>手順 12 を参照)、拒否されたトラフィックがログ ビューア</u> <u>に赤で表示されます。</u>より詳細なデバッグを取得するには、次のコマンドを実行します。

C:\WINNT\FW1\4.1\fwstop C:\WINNT\FW1\4.1\fw d -d **さらに、別のウィンドウで次のコマンドを実行します。**

C:\WINNT\FW1\4.1\fwstart 次のコマンドを実行すると、チェックポイントでセキュリティ アソシエーション(SA)をクリ アできます。

fw tab -t IKE_SA_table -x fw tab -t ISAKMP_ESP_table -x fw tab -t inbound_SPI -x fw tab -t ISAKMP_AH_table -x 「Are you sure?」というプロンプトには「yes」とプロンプトで表示されない場合があります。

<u>debug 出力例</u>

```
cisco_endpoint#vpn trac dump all
        4 seconds -- stepmngr trace enabled --
  new script: lan-lan primary initiator for <no id> (start)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
        38 seconds doing l2lp_init, (0 @ 0)
         38 seconds doing 121p_do_negotiation, (0 @ 0)
  new script: ISAKMP secondary Main for lan-lan-VPN0:1:[172.18.124.157] (start)
         38 seconds doing isa_i_main_init, (0 @ 0)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         38 seconds doing isa_i_main_process_pkt_2, (0 @ 0)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
        38 seconds doing isa_i_main_process_pkt_4, (0 @ 0)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing isa_i_main_process_pkt_6, (0 @ 0)
```

```
39 seconds doing isa_i_main_last_op, (0 @ 0)
   end script: ISAKMP secondary Main for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
   next script: lan-lan primary initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
        39 seconds doing l2lp_phase_1_done, (0 @ 0)
        39 seconds doing 121p_start_phase_2, (0 @ 0)
  new script: phase 2 initiator for lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing iph2_init, (0 @ 0)
        39 seconds doing iph2_build_pkt_1, (0 @ 0)
        39 seconds doing iph2_send_pkt_1, (0 @ 0)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
        39 seconds doing iph2_pkt_2_wait, (0 @ 0)
        39 seconds doing ihp2_process_pkt_2, (0 @ 0)
        39 seconds doing iph2_build_pkt_3, (0 @ 0)
        39 seconds doing iph2_config_SAs, (0 @ 0)
        39 seconds doing iph2_send_pkt_3, (0 @ 0)
        39 seconds doing iph2_last_op, (0 @ 0)
   end script: phase 2 initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
   next script: lan-lan primary initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
        39 seconds doing l2lp_open_tunnel, (0 @ 0)
        39 seconds doing l2lp_start_i_maint, (0 @ 0)
  new script: initiator maintenance for lan-lan-VPN0:1:[172.18.124.157] (start)
        39 seconds doing imnt_init, (0 @ 0)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
```

cisco_endpoint#**show vpn stat**

	Current	In	High	Running	Tunnel	Tunnel	Tunnel
	Active	Negot	Water	Total	Starts	OK	Error
Users	0	0	0	0	0	0	0
Partners	1	0	1	1	1	0	0
Total	1	0	1	1	1	0	0

IOP slot 1:

	Current	In Negot	High Water	Running Total	Tunnel Starts	Tunnel OK	Tunnel Error
Users	0	0	0	0	0	0	0
Partners	0	0	0	0	0	0	0
Total	0	0	0	0	0	0	0

cisco_endpoint#show vpn stat verb

	Current Active	In Negot	High Water	Running Total	Tunnel Starts	Tunnel OK	Tunnel Error
Users	0	0	0	0	0	0	0
Partners	1	0	1	1	1	0	0
Total	1	0	1	1	1	0	0

Stats	VPN0:1
Wrapped	13
Unwrapped	9
BadEncap	0
BadAuth	0
BadEncrypt	0
rx IP	9
rx IPX	0
rx Other	0
tx IP	13
tx IPX	0

tx Other	0						
IKE rekey	0						
Input VPN pkts dropped	due	to	no	SA:	0		
Input VPN pkts dropped	due	to	no	free	e queue	entries:	0
ISAKMP Negotiation stat	s						
Admin packets in	4						
Fastswitch packets in	0						
No cookie found	0						
Can't insert cookie	0						
Inserted cookie(L)	1						
Inserted cookie(R)	0						
Cookie not inserted(L)	0						
Cookie not inserted(R)	0						
Cookie conn changed	0						
Cookie already inserted	1 0						
Deleted cookie(L)	0						
Deleted cookie(R)	0						
Cookie not deleted(L)	0						
Cookie not deleted(R)	0						
Forwarded to RP	0						
Forwarded to IOP	0						
Bad UDP checksum	0						
Not fastswitched	0						
Bad Initiator cookie	0						
Bad Responder cookie	0						
Has Responder cookie	0						
No Responder cookie	0						
No SA	0						
Bad find conn	0						
Admin queue full	0						
Priority queue full	0						
Bad IKE packet	0						
No memory	0						
Bad Admin Put	0						
IKE pkt dropped	0						
No IIDP PBuf	0						
No Manager	0						
Mar w/ no cookie	0						
Cookie Scavence Add	1						
Cookie Scavence Rem	<u> </u>						
Cookie Scavenge Kem	0						
Cookie has mar orr	0						
Now conn limited	0						
Mem COURT TIULTED	U						

IOP slot 1:

	Current	In	High	Running	Tunnel	Tunnel	Tunnel
	Active	Negot	Water	Total	Starts	OK	Error
Users	0	0	0	0	0	0	0
Partners	0	0	0	0	0	0	0
Total	0	0	0	0	0	0	0

Stats Wrapped Unwrapped BadEncap BadAuth BadEncrypt rx IP

rx IPX

rx Other tx IP tx IPX tx Other IKE rekey Input VPN pkts dropped due to no SA: 0 Input VPN pkts dropped due to no free queue entries: 0 ISAKMP Negotiation stats Admin packets in 0 Fastswitch packets in 3 0 No cookie found Can't insert cookie 0 Inserted cookie(L) 0 Inserted cookie(R) 1 Cookie not inserted(L) 0 Cookie not inserted(R) 0 Cookie conn changed 0 Cookie already inserted 0 Deleted cookie(L) 0 Deleted cookie(R) 0 Cookie not deleted(L) 0 Cookie not deleted(R) 0 Forwarded to RP 0 Forwarded to IOP 3 Bad UDP checksum 0 Not fastswitched 0 Bad Initiator cookie 0 Bad Responder cookie 0 Has Responder cookie 0 No Responder cookie 0 No SA 0 Bad find conn 0 0 Admin queue full Priority queue full 0 Bad IKE packet 0 0 No memory Bad Admin Put 0 IKE pkt dropped 0 No UDP PBuf 0 No Manager 0 Mgr w/ no cookie 0 1 Cookie Scavenge Add 0 Cookie Scavenge Rem Cookie Scavenged 0 Cookie has mgr err 0 New conn limited 0



- 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 ネゴシエーション/IKE プロトコル
- ・ <u>テクニカル サポートとドキュメント Cisco Systems</u>