Cisco Secure PIX Firewall と Checkpoint NG Firewall 間のIPSec トンネル設定

内容

概要 前提条件 要件 <u>使用するコンポーネント</u> ネットワーク図 表記法 PIX の設定 Checkpoint NG の設定 確認 PIX 設定の検証 チェックポイントNGのトンネルステータスの表示 トラブルシュート PIX設定のトラブルシューティング ネットワーク集約 チェックポイントNGログの表示 関連情報

概要

このドキュメントでは、2 つのプライベート ネットワーク間で通信するために事前共有キーを使 用して IPSec トンネルを設定する方法について説明します。この例では、通信するネットワーク は、Cisco Secure PIX Firewall 内部の 192.168.10.x プライベート ネットワークと Checkpoint(TM) Next Generation(NG)ファイアウォール内部の 10.32.x.x プライベート ネット ワークです。

前提条件

<u>要件</u>

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。

- ●この設定を開始する前に、PIX内部および^{Checkpoint™} NG内部からインターネット(ここでは 172.18.124.xネットワークで表されます)へのトラフィックが流れる必要があります。
- ユーザが IPsec のネゴシエーションに精通している必要があります。このプロセスは、2つの インターネットキー交換(IKE)フェーズを含む5つのステップに分けることができます。対象 トラフィックによって IPsec トンネルが開始されます。IPsec ピアの間を転送されるトラフ

ィックは、対象トラフィックとみなされます。IKE フェーズ 1 では、IPsec ピア同士が、IKE セキュリティ アソシエーション (SA) ポリシーについてネゴシエートします。ピアが認証さ れると、Internet Security Association and Key Management Protocol (ISAKMP)を使用して 安全なトンネルが作成されます。IKE フェーズ 2 では、IPsec ピア同士が認証済みの安全な トンネルを使用して、IPsec SA トランスフォームをネゴシエートします。共有ポリシーのネ ゴシエーションによって、IPsec トンネルの確立方法が決まります。IPsec トンネルが作成さ れ、IPsec トランスフォーム セットに設定された IPsec パラメータに基づいて、IPsec 間で データが伝送されます。IPsec SA が削除されるか、そのライフタイムの有効期限が切れると 、IPsec トンネルは終了します。

<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。

- PIX ソフトウェア リリース 6.2.1
- ・^{CheckpointTM NGファ}イアウォール

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>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>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』を参照してください。</u>

<u>PIX の設定</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の情報を提供します。

PIX の設定
PIX Version 6.2(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIXRTPVPN

domain-name cisco.com fixup protocol ftp 21 fixup protocol http 80 fixup protocol h323 h225 1720 fixup protocol h323 ras 1718-1719 fixup protocol ils 389 fixup protocol rsh 514 fixup protocol rtsp 554 fixup protocol smtp 25 fixup protocol sqlnet 1521 fixup protocol sip 5060 fixup protocol skinny 2000 names !--- Interesting traffic to be encrypted to the Checkpoint™ NG. access-list 101 permit ip 192.168.10.0 255.255.255.0 10.32.0.0 255.255.128.0 !--- Do not perform Network Address Translation (NAT) on traffic to the Checkpoint™ NG. access-list nonat permit ip 192.168.10.0 255.255.255.0 10.32.0.0 255.255.128.0 pager lines 24 interface ethernet0 10baset interface ethernet1 10full mtu outside 1500 mtu inside 1500 ip address outside 172.18.124.158 255.255.255.0 ip address inside 192.168.10.1 255.255.255.0 ip audit info action alarm ip audit attack action alarm pdm history enable arp timeout 14400 global (outside) 1 interface !--- Do not perform NAT on traffic to the Checkpoint™ NG. nat (inside) 0 access-list nonat nat (inside) 1 0.0.0.0 0.0.0.0 0 0 route outside 0.0.0.0 0.0.0.0 172.18.124.1 1 timeout xlate 3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00h323 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 aaa-server LOCAL protocol local no snmp-server location no snmp-server contact snmp-server community public no snmp-server enable traps floodguard enable !--- Permit all inbound IPsec authenticated cipher sessions. sysopt connection permit-ipsec no sysopt route dnat !--- Defines IPsec encryption and authentication algorithms. crypto ipsec transform-set rtptac esp-3des esp-md5-hmac !--- Defines crypto map. crypto map rtprules 10 ipsecisakmp crypto map rtprules 10 match address 101 crypto map rtprules 10 set peer 172.18.124.157 crypto map rtprules 10 set transform-set rtptac !--- Apply crypto map on the outside interface. crypto map rtprules interface outside isakmp enable outside !--- Defines pre-shared secret used for IKE authentication. isakmp key ******* address

```
172.18.124.157 netmask 255.255.255.255

!--- Defines ISAKMP policy. isakmp policy 1

authentication pre-share

isakmp policy 1 encryption 3des

isakmp policy 1 hash md5

isakmp policy 1 group 2

isakmp policy 1 lifetime 86400

telnet timeout 5

ssh timeout 5

terminal width 80

Cryptochecksum:089b038c8e0dbc38d8ce5ca72cf920a5

: end
```

<u>Checkpoint NG の設定</u>

^{CheckpointTM} NGでネットワークオブジェクトとルールが定義され、設定するVPN設定に関連する ポリシーが作成されます。このポリシーは、^{CheckpointTM} NG Policy Editorを使用してインストー ルされ、構成の^{CheckpointTM} NG側を完了します。

 対象トラフィックを暗号化するCheckpointネットワークとPIX Firewallネットワークの2つの ネットワークオブジェクトを作成します。これを行うには、[Manage] > [Network Objects]の 順に選択し、[New] > [Network]を選択します。適切なネットワーク情報を入力して、[OK] を クリックします。次の例は、CP_Inside(^{CheckpointTM} NGの内部ネットワーク)および PIXINSIDE(PIXの内部ネットワーク)と呼ばれるネットワークオブジェクトのセットを示 しています。

Network Prope	rties - CP_inside	×
General NAT		
<u>N</u> ame:	CP_inside	
IP <u>A</u> ddress:	10.32.0.0	
Net <u>M</u> ask:	255.255.128.0	
<u>C</u> omment:	CPINSIDE	
Co <u>l</u> or:		
Broadcast Includ	t address: ed ON <u>o</u> t included	
	OK Cancel Help	

Network Prope	rties - PIXINSIDE		×
General NAT]		
<u>N</u> ame:	PIXINSIDE		
IP <u>A</u> ddress:	192.168.10.0		
Net <u>M</u> ask:	255.255.255.0		
<u>C</u> omment:	Pixinside		
Co <u>l</u> or:			
Broadcas <u>I</u> nclud	t address: ed <u>O No</u> t included		
	OK Cancel Help	>	

2. CheckpointTM NGおよびPIX用のワークステーショ^{ンのオブジェ}クトを作成します。これを行 うには、[Manage] > [Network Objects] > [New] > [Workstation] の順に選択します。 Checkpoint^{TM NG の初期設定の際に作成した CheckpointTM NG ワークステーション オブジェクトを使用でき ^{ます。}ワークステーションをゲートウェイおよび相互運用可能VPNデバイスとして設定する オプションを選択し、[OK]をクリックします。次の例は、ciscocp(CheckpointTM NG)および PIX(PIX Firewall)と呼ばれるオブジェクトのセットを示しています。}

Workstation Properties - o	ciscocp			×
Workstation Properties - o General Topology NAT VPN Authentication Management II - Advanced	ciscocp General Name: IP Address: Color: Type:	ciscocp 172.18.124.157 Checkpoint External IP C Host © Gateway	<u>G</u> et address	X
	Check Point	Products int products installed: Version NG ireWall-1 o-1 ver anagement Station	i 🔽 Get Version]]
	Object Managed Managed Secure Interr Communic	gement	al) xtemal) cocppvzfoa	
		ОК	Cancel	Help

Workstation Properties -	PIX			×
General	General			
- NAT	<u>N</u> ame:	PIX		
	IP <u>A</u> ddress:	172.18.124.158	<u>G</u> et address	
	<u>C</u> omment:	PIX Firewall		
	Color:			
	Type:	⊂ <u>H</u> ost		
	Check Point f	Products		
	Check Po	int products installed: Version NG	i 💌 Get Version	
	□VPN-1 & F □FloodGate □Policy Ser □Managem	fireWall-1 ⊶1 ver ent Station	•	
	Object Manag	gement		
	C Managed	by this Management Server [Intern	al)	
	C Managed	by another Management Server (E)	ktemal)	
	✓ Interope	rable ⊻PN Device		
,		OK	Cancel	Help

[Manage] > [Network objects] > [Edit] を選択し、CheckpointTM NGワークステーション(この例ではciscocp)の[Workstation Properties]ウィンドウを開きます。ウィンドウの左側の選択肢から[Topology]を選択し、暗号化するネットワークを選択します。[編集]をクリックして、インターフェイスのプロパティを設定します。

Workstation Properties - o	iscocp				×
- General Topology	Topology Get Interfaces	1			
		1			
Authentication	Name	IP Address	Network Mask	IP Addresses behind	
Management	E100B0	10.32.50.50	255.255.128.0	CP_inside	
⊕-Advanced	ETUUBT	172.18.124.157	255.255.255.0	External	
	•				
	Add Show all IPs beh VPN Domain All IP Addresse information. Manually Defin	Edit	<u>Remove</u>	Show Show Show	
			ок	Cancel Help	

4. ワークステーションを内部として指定するオプションを選択し、適切なIPアドレスを指定し ます。[OK] をクリックします。この設定では、CP_insideはCheckpointTM NGの内部ネット ワーク^です。ここに示すトポロジ選択では、ワークステーションを内部として指定し、アド レスをCP_insideとして指定します。

1	Interface Properties	×
	General Topology QoS	
	Topology	
	<u>External (leads out to the internet)</u>	
	 Internal (leads to the local network) 	
	IP Addresses behind this interface:	
	O <u>N</u> ot Defined	
	O Network defined by the interface IP and Net Mask	
	Anti-Spoofing ✓ Perform Anti-Spoofing based on interface topology Spoof Tracking: ○ None ⓒ Log ○ Alert	
	OK Cancel Help	

5. [Workstation Properties]ウィンドウで、インターネットに接続する^{CheckpointTM} NGの外部イ ンターフェイスを選択し、[Edit]をクリックしてインターフェイスのプロパティを設定しま す。トポロジを外部として指定するオプションを選択し、[OK]をクリ**ックします**。

Interface Properties 🛛 🗙
General Topology QoS
External [leads out to the internet]
Internal (leads to the local network)
IP Addresses behind this interface:
C Not Defined
C Network defined by the interface IP and Net Mask
O <u>S</u> pecific:
Anti-Spoofing
And opcoming
Perform Anti-Spoofing based on interface topology
Spoof Tracking: O None O Log O Alert
OK Cancel Help
OK Cancel Help

6. CheckpointTM NGのWorkstation Propertiesウィンドウで、ウィンドウの左側にある選択肢から VPNを選択し、次に暗号化および認証アルゴリズムのIKEパラメータを選択します。[Edit]を クリックしてIKEプロパティを設定します。

Workstation Properties - o	iscocp			×
General Topology NAT VPN Authentication Management € Advanced	VPN Encryption schemes	set default <u>I</u> KE pro	operties	
	Nickname DN ▲dd	Edit	Certificate Authority	

 IKEプロパティを設定します。3DES暗号化のオプションを選択して、IKEプロパティが isakmp policy # encryption 3desコマンドと互換性を持つようにします。IKEプロパティが crypto isakmp policy # hash md5コマンドと互換性を持つように、MD5のオプションを選択

IKE Properties	×
General	
Support key exchange encryption	with: Support data integrity with:
DES	▲ <u>MD5</u>
CAST	
Support authentication methods: -	
☑ Pre-Shared Secret	Edit <u>S</u> ecrets
Public Key Signatures	Specify
□	ation for SecuRemote (Hybrid Mode)
	<u>A</u> dvanced
	ancel Help

します。 느

8. Pre-Shared Secretsの認証オプションを選択し、Edit Secretsをクリックして、事前共有キー をPIXコマンドisakmp key address address netmask netmaskと互換性があるように設定し ます。[Edit]をクリックして、ここに示すようにキーを入力し、[Set]、[OK]の順にクリック

-	Shar	ed Secret				×
	۲ ⁹	Shared Secrets Lis	t:			
		Peer Name	Shared Secre	t 📃		
		PIX	****		<u>E</u> dit	
					Bemove	1
					<u></u>	1
		Enter secret: cis	cortp	Set		
đ		ОК	Cancel		<u>H</u> elp	

します。

9. IKEプロパティウィンドウで、[Advanced...]をクリックし、次の設定を変更します。「アグ レッシブモードをサポート」のオプションを選択解除します。[サブネットのキー交換をサ ポートする]オプションを選択します。完了したら、[OK] をクリックします。

Advanced IKE properties			×
Use <u>U</u> DP encapsulation	UDP VPN1_IPSE	:C_encapsi 💌	
Support Diffie-Hellman groups			
	Group 1 (768 ✓ Group 2 (1024 Group 5 (1538	bit) 4 bit) 5 bit)	
Rekeying Parameters			
Renegotiate IKE security associa	tions	1440 🔅	Minutes
Renegotiate IPSEC Security asso	ciations every	3600 🗧	Seconds
Renegotiate IPSEC Security a	associations every	50000 🚔	KBytes
Misc Support IP <u>c</u> ompression for Se Support <u>agg</u> resive mode Support key exchange for <u>s</u> ut	ecureClient onets		
OK C	ancel	<u>H</u> elp	

10. [Manage] > [Network objects] > [Edit] を選択して、PIXの[Workstation Properties]ウィンド ウを開きます。ウィンドウの左側の選択肢から**[Topology]**を選択し、VPNドメインを手動 で定義します。この設定では、PIX内部ネットワーク(PIXの内部ネットワーク)がVPNド メインとして定義されています。

Workstation Properties - I	XIX				×
General	Topology				
Topology - NAT	<u>G</u> et Interfaces				
VPN	Name	IP Address	Network Mask		
Advanced					
	,		Ramon 1 - 4	2ham I	
		Editor.	Tellove 3	27(3/4)	
	Show all IPs behi	nd Gateway			
	VPN Domain				-
	 All IP Addresses information. 	s <u>b</u> ehind Gateway ba	ased on Topology	Sh <u>o</u> w	
	Manually Define		•	Sho <u>w</u>	
	Exportable for S	ecuRemote.			
		courremote			
		_			- (
			OK C	ancel Help)

11. ウィンドウの左側**の選択肢**から[VPN]を選択し、暗号化方式として[IKE]を選択します。 [**Edit**]をクリックしてIKEプロパティを設定します。

Workstation Properties -	PIX			×
General Topology NAT Advanced	VPN Encryption schemes			
		OK	Cancel H	elp

12. 次のようにIKEプロパティを設定します。3DES暗号化のオプション**を選択し**て、IKEプロ パティがisakmp policy # encryption 3desコマンドと互換性**を持つようにします**。IKEプロ パティが**crypto isakmp policy # hash md5**コマンドと互換性を持つように、MD5のオ**プショ**

IKE Properties General	
Support key exchange encryption	n with:
 Support authentication methods: Pre-Shared Secret Rublic Key Signatures 	Edit <u>S</u> ecrets
Public <u>N</u> ey Signatures	ication for SecuRemote (Hybrid Mode)
	<u>A</u> dvanced
ОК	Cancel Help

ンを選択します。

13. Pre-Shared Secretsの認証オプションを選択し、Edit Secretsをクリックして、事前共有キ ーをPIXコマンドisakmp key address address netmask netmaskと互換性があるように設定 します。[Fdit]をクリックしてキーを入力し、[Set]、[OK]の順にクリックします。

			<u> </u>		///
Share	ed Secret				×
_9	Shared Secrets List: -				
	Peer Name	Shared Secret			
	ciscocp	****		<u>E</u> dit	
				Bemaua	
	,				
		Cancel	1 г	Help	

14. IKEプロパティウィンドウで、[Advanced...]をクリックして、これらの設定を変更します。 IKEプロパティに適したDiffie-Hellmanグループを選択します。「アグレッシブモードをサ ポート」のオプションを選択解除します。[サブネットのキー交換をサポートする]オプショ ンを選択します。完了したら、[OK]、[OK]の順にクリックします。

Advanced IKE properties			×
Use UDP encapsulation			
	UDP VPN1_IPSE	:C_encapsi 🔽	
Support Diffie-Hellman groups			
	Group 1 (768	bit)	
	Group 5 (1536	F Dit) S bit)	
	J		
Rekeying Parameters			
Renegotiate IKE security associat	ions	1440 🗦	Minutes
Renegotiate IPSEC Security asso	ciations every	3600 🗦	Seconds
🔲 Renegotiate IPSEC Security a	ssociations every	50000 🛓	KBytes
Wi			
MISC -	ouroCliept		
Support aggresive mode	conconent.		
Support key exchange for sub	inets		
	ancel	Help	

15. [Rules] > [Add Rules] > [Top] を選択して、ポリシーの暗号化ルールを設定します。Policy Editorウィンドウで、送信元と宛先の両方のカラムにCP_inside(Checkpoint TM NGの内部 ネットワーク)とPIXINSIDE (PIXの内部ネットワーク)のソースを持つルールを挿入しま す。Service = **Any、Action = Encrypt、Track = Logの値を設定します**。ルールの[Encrypt Action]セクションを追加したら、[Action]を右クリック」、[Edit Proportios]を選択します

Action」ビフションを進	ョ加したら、[ACII	の心をロント	550	[⊏aii Properii	<u>es</u>]で医外	しまり。			
CISCOCP - Check Point Policy Editor	- Standard								
File Edit View Manage Rules Policy	Topology Search Window He	¢							
№ @ @ 0 0 0 0.	🕹 🙀 🖄 🛞 💾 🔗 🔗 🔍 🗰 Security - Standard 🗱 Address Translation - Standard 🗰 QoS - Standard 🛍 Desitop Security - Standard								
E- La Network Objects	NO. SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL			
- L discorp									
I PEK	1 4 CP_Inside 4 PRINSIDE	CP_inside	🗙 Any	Edit propert	5es	🔝 Gateway:			
B Network	2 H CE inside	+ Anv	· ànu	Add Endryp		Codeward			
Provision		 Out 	• Aug	Water Contenting		C Oateway:			
Domain				😗 accept					
OSE Device				irop 🥘					
Embedded Device				reject					
- III Group				😂 User Auth					
Logical Server	1			Client Aut					
Address Range				😑 Session A	wth	<u>.</u> .			
Dynamic Object	Name	DP	Comment	Encrypt					
and a product output	ciscocp	172.10.1	24.157 Chedipoin	t External I 🙆 Client Encr	typt				
	II PIX	172.18.1	24.158 PDX Firewa						
	1			Query Colu	80				
				Clear Query					

16. [IKE] が選択され、強調表示された状態で、[Edit] をクリックします。

Encryption Properties			×
General			
Encryption <u>s</u> chemes define	ed:		
🕅 📷 IKE 💭 💑 FWZ			
<u> </u>			
ОК	Cancel	Help	

17. [IKE Properties]ウィンドウで、crypto ipsec transform-set rtptac esp-3des esp-md5-hmacコ マンドのPIX IPSecトランスフォームと一致するようにプロパティを変更します。 TransformオプションをEncryption + Data Integrity(ESP)に設定し、Encryption Algorithmを

3DESに設定し、Data IntegrityをMD5に設定し、Allowed Peer Gatewayを外部PIXゲートウェイとと一致に設定します(ここで呼呼します)。 [OK] をクリックします。

IKE Properties	×
General	
Transform	
Encryption + Data Integrity	(ESP)
O Data Integrity Only (AH)	
Encryption Algorithm:	3DES 💌
<u>D</u> ata Integrity	MD5
<u>Compression method:</u>	None
<u>A</u> llowed Peer Gateway:	PIX 💌
Use Perfect Forward Secrecy	
Use DH <u>G</u> roup:	
Perform IP Pool NAT	
OK Ca	ncel Help

18. CheckpointTM NGを設定した後、ポリシーを保存し、[**Policy**] > [**Install**]を選択して有効にします。

CISCOCP - Check Point Policy	Editor - Standard					_ [] X				
File Edit View Manage Rules	Policy Topology Search Window	Help								
日 シ X 1 1 4	Verify Install	°≘∃≪ ♥	54 S							
°ta 💼 📰 🌮 🛃 🚦	Uninstall	0								
º € < © 8 0	Access Lists	Address Translation - Standard 🗱 QoS - Standard 🎦 Desktop Security - Standard								
Ketwork Objects Workstation	Install Users Database	DESTINATION	SERVICE	ACTION	TRACK	INSTALL				
ciscocp	Global Properties	부 POINSIDE 부 CP_inside	* Any	Encryst	🔳 Log	Gaterway:				
B Metwork	2 🕂 OP_inside	* Any	* Any	@ eccept	E Log	Gateway:				
- PDGNSIDE										
OSE Device										
Embedded Device										
Group										
- PR Address Range						101				
Gateway Cluster		1	ana a ar							
- Dynamic Object	Name	1	Convient							
_	ciscocp	172.18.1	24.157 Checkpoi	nt External IP						
	D PDC	172,18,1	24.158 PEX Firew	al						
	CP_inside	10.32.0.	0 OPINSIDE	5						
	PDUNSIDE	192.168	10.0 Poinside							

ポリシーがコンパイルされるときには、インストレーション ウィンドウに進捗状態が表示 されます。

			V
Install Policy			Ň
Standard.W: Security Po Standard: Compiled OK.	licy Script generated	into Standard.pf	×
			▶
		rt)	

トールウィンドウに、ポリシーのインストールが完了したことが示された場合。[閉じる]**を** クリックして、手順を終了します。



<u>確認</u>

<u>PIX 設定の検証</u>

ここでは、設定が正常に機能しているかどうかを確認します。

<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。

2つのプライベートネットワーク間の通信をテストするために、プライベートネットワークの1つ から他のプライベートネットワークへのpingを開始します。この設定では、pingがPIX側 (192.168.10.2)から^{CheckpointTM} NG内部ネットワーク(10.32.50.51)に送信されました。

• show crypto isakmp sa:現在ピアにあるすべての IKE SA を表示します。

show crypto isakmp sa Total : 1 Embryonic : 0 dst. state pending created src 172.18.124.158 QM_IDLE 172.18.124.157 0 1 show crypto ipsec sa:現在の SA で使用されている設定を表示します。 PIX501A#show cry ipsec sa interface: outside Crypto map tag: rtprules, local addr. 172.18.124.158 local ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (10.32.0.0/255.255.128.0/0/0) current_peer: 172.18.124.157 PERMIT, flags={origin_is_acl,} #pkts encaps: 19, #pkts encrypt: 19, #pkts digest 19 #pkts decaps: 19, #pkts decrypt: 19, #pkts verify 19 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0 #send errors 1, #recv errors 0

```
local crypto endpt.: 172.18.124.158, remote crypto endpt.: 172.18.124.157
path mtu 1500, ipsec overhead 56, media mtu 1500
current outbound spi: 6b15a355
inbound esp sas:
spi: 0xced238c7(3469883591)
   transform: esp-3des esp-md5-hmac ,
  in use settings ={Tunnel, }
  slot: 0, conn id: 3, crypto map: rtprules
  sa timing: remaining key lifetime (k/sec): (4607998/27019)
  IV size: 8 bytes
  replay detection support: Y
inbound ah sas:
inbound pcp sas:
outbound esp sas:
spi: 0x6b15a355(1796580181)
  transform: esp-3des esp-md5-hmac ,
  in use settings ={Tunnel, }
  slot: 0, conn id: 4, crypto map: rtprules
  sa timing: remaining key lifetime (k/sec): (4607998/27019)
  IV size: 8 bytes
  replay detection support: Y
outbound ah sas:
```

outbound pcp sas:

<u>チェックポイントNGのトンネルステータスの表示</u>

Policy Editorに移動し、Window > System Statusの順に選択してトンネルのステータスを表示します。

😴 CISCOCP - Check Point System Status									
<u>File View M</u> odules <u>P</u> roducts <u>T</u> ools <u>W</u> indow <u>H</u> elp									
) 🗩 🕒 🗛 👖 🔦 🚥 🗞 📾 🚅 🎯 😤	\$?								
Modules IP Address	VPN-1 Details								
	Status: OK								
È I iscocp 172.18.124.157	Packets								
FireWall-1	Encrypted: 20								
FloodGate-1	Decrypted: 20								
Management	Errors								
SVN Foundation	Encryption errors: 0								
VFN-1	Decryption errors: 0								
	IKE events errors: 0								
	Hardware								
	HW Vendor Name: none								
	HW Status: none								

<u>トラブルシュート</u>

<u>PIX設定のトラブルシューティング</u>

<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。

次のコマンドを使用して、PIX Firewallのデバッグを有効にします。

- ・debug crypto engine:暗号化と復号化を行う暗号化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。

VPN Peer: ISAKMP: Added new peer: ip:172.18.124.157 Total VPN Peers:1
VPN Peer: ISAKMP: Peer ip:172.18.124.157 Ref cnt incremented to:1 Total VPN Peers:1
ISAKMP (0): beginning Main Mode exchange
crypto_isakmp_process_block: src 172.18.124.157, dest 172.18.124.158
OAK_MM exchange
ISAKMP (0): processing SA payload. message ID = 0
ISAKMP (0): Checking ISAKMP transform 1 against priority 1 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80
ISAKMP (0): atts are acceptable. Next payload is 0
ISAKMP (0): SA is doing pre-shared key authentication using id type ID_IPV4_ADDR

return status is IKMP_NO_ERROR crypto_isakmp_process_block: src 172.18.124.157, dest 172.18.124.158 OAK_MM exchange ISAKMP (0): processing KE payload. message ID = 0 ISAKMP (0): processing NONCE payload. message ID = 0 ISAKMP (0): ID payload next-payload : 8 type : 1 protocol : 17 port : 500 length : 8 ISAKMP (0): Total payload length: 12 return status is IKMP_NO_ERROR crypto_isakmp_process_block: src 172.18.124.157, dest 172.18.124.158 OAK_MM exchange ISAKMP (0): processing ID payload. message ID = 0 ISAKMP (0): processing HASH payload. message ID = 0 ISAKMP (0): SA has been authenticated ISAKMP (0): beginning Quick Mode exchange, M-ID of 322868148:133e93b4 IPSEC(key_engine): got a queue event... IPSEC(spi_response): getting spi 0xced238c7(3469883591) for SA from 172.18.124.157 to 172.18.124.158 for prot 3 return status is IKMP_NO_ERROR ISAKMP (0): sending INITIAL_CONTACT notify ISAKMP (0): sending NOTIFY message 24578 protocol 1 ISAKMP (0): sending INITIAL_CONTACT notify crypto_isakmp_process_block: src 172.18.124.157, dest 172.18.124.158 OAK_QM exchange oakley_process_quick_mode: OAK_QM_IDLE ISAKMP (0): processing SA payload. message ID = 322868148 ISAKMP : Checking IPSec proposal 1 ISAKMP: transform 1, ESP_3DES ISAKMP: attributes in transform: ISAKMP: encaps is 1 ISAKMP: SA life type in seconds ISAKMP: SA life duration (basic) of 28800 ISAKMP: SA life type in kilobytes ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 ISAKMP: authenticator is HMAC-MD5 ISAKMP (0): atts are acceptable. IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) dest= 172.18.124.157, src= 172.18.124.158, dest_proxy= 10.32.0.0/255.255.128.0/0/0 (type=4), src_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 ISAKMP (0): processing NONCE payload. message ID = 322868148 ISAKMP (0): processing ID payload. message ID = 322868148 ISAKMP (0): processing ID payload. message ID = 322868148 ISAKMP (0): processing NOTIFY payload 24576 protocol 3 spi 3469883591, message ID = 322868148 ISAKMP (0): processing responder lifetime ISAKMP (0): processing NOTIFY payload 24576 protocol 3 spi 3469883591, message ID = 322868148 ISAKMP (0): processing responder lifetime ISAKMP (0): Creating IPSec SAs inbound SA from 172.18.124.157 to 172.18.124.158 (proxy 10.32.0.0 to 192.168.10.0) has spi 3469883591 and conn_id 3 and flags 4 lifetime of 28800 seconds lifetime of 4608000 kilobytes outbound SA from 172.18.124.158 to 172.18.124.157 (proxy 192.168.10.0 to 10.32.0.0) has spi 1796580181 and conn_id 4 and flags 4 lifetime of 28800 seconds

lifetime of 4608000 kilobytesIPSEC(key_engine): got a queue event... IPSEC(initialize_sas): , (key eng. msg.) dest= 172.18.124.158, src= 172.18.124.157, dest_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4), src_proxy= 10.32.0.0/255.255.128.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 28800s and 4608000kb, spi= 0xced238c7(3469883591), conn_id= 3, keysize= 0, flags= 0x4 IPSEC(initialize_sas): , (key eng. msg.) src= 172.18.124.158, dest= 172.18.124.157, src_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4), dest_proxy= 10.32.0.0/255.255.128.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 28800s and 4608000kb, spi= 0x6b15a355(1796580181), conn_id= 4, keysize= 0, flags= 0x4 VPN Peer: IPSEC: Peer ip:172.18.124.157 Ref cnt incremented to:2 Total VPN Peers:1 VPN Peer: IPSEC: Peer ip:172.18.124.157 Ref cnt incremented to:3 Total VPN Peers:1 return status is IKMP_NO_ERROR

<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。PIXの暗号アクセスコントロールリスト(ACL)が一致するように設定されていない場 合、トンネルは失敗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、それらを10.0.0.0 /23に集約できます。

<u>チェックポイントNGログの表示</u>

[Window] > [Log Viewer]を選択して、ログを表示します。

	CISCOCP - C	heck Poir	ıt Log Vie	wer - [[w.log]		1 - 81			ō · → i+ i+ i+ i+ i+ i+ i+ i+ i	-1	
64	e Mode Ed	k Selectio	n Yee	Icois)	Mindow 🖯	de qe						
É	9 🤹 🖬	Log	*	+ 4	(¥ 🕇	۵ ک	% 👼	· 📄 🗰 📴	🇞 🔛 😘	8 O I	1	
11	Date	Time	Product		Inter.	Orig	Туре	Action	Source	Destina	.	nto.
0	23Aug2002	17:32:47	VPN-1	8 Firel/V	kall 💽 da.	. ciscoop	🔳 log	Ow key install	POC	ciscoop		KE: Main Mode completion.
t.	23Aug2002	17:32:47	VPN-4	& FireW	kil 💽 de.	. ciscoop	📕 log	Oray key install	POC	ciscocp		IKE: Quick Mode Received Notification from Peer: Initial Contact
2	23Aug2002	17:32:47	W VPN-1	& Firel/V	kil 💽 da.	. ciscoop	🔳 log	0-e key install	PK	ciscocp		IKE: Guick Mode completion IKE IDs: subnet: 10.32.0.0 (mest= 255.25
з	23Aug2002	17:32:48	W VPN-1	& Firel/V	kal 💽 Et.	. ciscoop	🔳 log	😡 decrypt	192:168 10:2	10.32.50.51 (0	icmp-type 8 icmp-code 8
4	23Aug2002	17:32:48	VPN-1	& Firel/V	NI 💽 E1.	. ciscoop	📕 log	🚘 decrypt	192.168.10.2	10.32.50.51 (0	icmp-type 8 icmp-code 0
5	23Aug2002	17:32:48	WEN-1	& Firel/V	MI 💽 E1.	. clecoop	109	😡 decrypt	192:168:10:2	10.32.50.51	0	icmp-type 8 icmp-code 0
6	23Aug2002	17:32:48	VPN-1	& Firel/V	lal 💽 (;1.	. ciscoop	🔳 log	🔒 decrypt	192.168.10.2	10.32.50.51 (0	icmp-type 8 icmp-code 8

<u>関連情報</u>

- <u>Cisco PIX Firewall ソフトウェア</u>
- Cisco Secure PIX ファイアウォール コマンド リファレンス
- セキュリティ製品に関する Field Notice (PIX を含む)
- <u>Requests for Comments (RFCs)</u>
- <u>テクニカル サポートとドキュメント Cisco Systems</u>