Cisco VPN 3000 コンセントレータと 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> 表記法 ネットワーク図 設定 VPN 3000 コンセントレータの設定 Checkpoint NG の設定 確認 ネットワーク通信の確認 チェックポイントNGのトンネルステータスの表示 VPNコンセントレータのトンネルステータスの表示 トラブルシュート <u>ネットワー</u>ク集約 チェックポイントNG のデバッグ VPN コンセントレータのデバッグ 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 VPN 3000 コンセントレータ内部の 192.168.10.x プライベート ネットワークと Checkpoint 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。

<u>前提条件</u>

<u>要件</u>

- VPNコンセントレータ内部および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る)へのトラフィックは、この設定を開始する前にフロー する必要があります。
- ユーザはIPSec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 Security Association (SA; セキュリティ結合) 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 用してセキュアトンネルが作成されます。IKEフェーズ2では、IPSecピアは、IPSec SAトラ ンスフォームをネゴシエートするために、認証された安全なトンネルを使用します。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で設定されたIPSecパラメータに基づいて、 IPSecピア間でデータが転送されます。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>

この設定は、次のバージョンのソフトウェアとハードウェアを使用して作成およびテストされて います。

- VPN 3000シリーズコンセントレータ3.5.2
- Checkpoint NG Firewall

<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>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。



注:この設定で使用されるIPアドレッシング方式は、インターネット上で正式にルーティング可能なものではありません。これらはラボ環境で使用された RFC 1918 のアドレスです。

<u>設定</u>

<u>VPN 3000 コンセントレータの設定</u>

VPN 3000コンセントレータを設定するには、次の手順を実行します。

 [Configuration] > [System] > [Tunneling Protocols] > [IPSec LAN-to-LAN]に移動して、LANto-LANセッションを設定します。認証およびIKEアルゴリズム、事前共有キー、ピアIPアド レス、ローカルおよびリモートネットワークパラメータのオプションを設定します。[Apply] をクリックします。この設定では、認証はESP-MD5-HMACに設定され、暗号化は3DESに

<u>設定されています。</u>

Configuration System Tunneling Protocols IPSec LAN-to-LAN Modify			
Modify an IPSec LAN-to-LAN connection.			
Nama Chastasiat	Enter the name for this I AN to J AN connection		
Transe Checkpoint	Enter the name for this LAN-to-LAN connection.		
Interface Ethernet 2 (Public) (172.18.124.131)	Select the interface to put this LAN-to-LAN connection on.		
Peer 172.18.124.157	Enter the IP address of the remote peer for this LAN-to-LAN connection.		
Digital None (Use Preshared Keys) Certificate	Select the Digital Certificate to use.		
Certificate Certi	Choose how to send the digital certificate to the IKE peer.		
Preshared Key ciscortprules	Enter the preshared key for this LAN-to-LAN connection.		
Authentication ESP/MD5/HMAC-128 ·	Specify the packet authentication mechanism to use.		
Encryption 3DES-168	Specify the encryption mechanism to use.		
IKE Proposal IKE-3DES-MD5	Select the IKE Proposal to use for this LAN-to-LAN connection.		
Routing None	Choose the routing mechanism to use.Parameters below are ignored if Network Autodiscovery is chosen.		
Local Network			
Network List Use IP Address/Wildcard-mask below -	Specify the local network address list or the IP address and wildcard mask for this LAN-to-LAN connection.		
IP Address 192.168.10.0	Note: Enter a wildcard mask, which is the reverse of a subnet mask. A		
Wildcard Mask 0.0.0.255	wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.		
Remote Network			
Network List Use IP Address/Wildcard-mask below	Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection.		
IP Address 10.32.0.0	Note: Enter a <i>wildcard</i> mask, which is the reverse of a subnet mask. A		
Wildcard Mask 0.0.127.255	wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.		
Apply Cancel			

 Configuration > System > Tunneling Protocols > IPSec > IKE Proposalsの順に選択し、必要 なパラメータを設定します。IKEプロポーザルIKE-3DES-MD5を選択し、プロポーザルに対 して選択されたパラメータを確認します。[Apply]をクリックして、LAN-to-LANセッション を設定します。この設定のパラメータは次のとおりです。

Configuration System Tunneling Protocols IPSec IKE Proposals Modify				
Modify a configured IKE Proposal.				
Proposal Name IKE-3DES-MD5	Specify the name of this IKE Proposal.			
Authentication Mode Preshared Keys	 Select the authentication mode to use. 			
Authentication Algorithm MD5/HMAC-128 -	Select the packet authentication algorithm to use.			
Encryption Algorithm 3DES-168 -	Select the encryption algorithm to use.			
Diffie-Hellman Group Group 2 (1024-bits) 💌	Select the Diffie Hellman Group to use.			
Lifetime Measurement Time 💌	Select the lifetime measurement of the IKE keys.			
Data Lifetime 10000	Specify the data lifetime in kilobytes (KB).			
Time Lifetime 86400	Specify the time lifetime in seconds.			
Apply Cancel				

3. [Configuration] > [Policy Management] > [Traffic Management] > [Security Associations] に移 動し、セッション用に作成されたIPSec SAを選択し、LAN-to-LANセッション用に選択され たIPSec SAパラメータを確認します。この設定では、LAN-to-LANセッション名は「 Checkpoint」であるため、IPSec SAは自動的に「L2L:チェックポイント。」

Configuration | Policy Management | Traffic Management | Security Associations

Save Needed

This section lets you add, configure, modify, and delete IPSec Security Associations (SAs). Security Associations use IKE Proposals to negotiate IKE parameters.

Click Add to add an SA, or select an SA and click Modify or Delete.

IPSec SAs	Actions
ESP-DES-MD5	
ESP-3DES-MD5	
ESP/IKE-3DES-MD5	0.44
ESP-3DES-NONE	Add
ESP-L2TP-TRANSPORT	Modify
ESP-3DES-MDS-DH7	
L2L. Glieuxpoint	Delete

このSAのパラメータは次のとおりです。

Configuration Policy Management Traffic Management Security Associations Modify				
Modify a configured Security Association.				
SA Name L2L: Checkpoint Inheritance From Rule •	Specify the name of this Security Association (SA). Select the granularity of this SA.			
IPSec Parameters Authentication Algorithm ESP/MD5/HMAC-128 • Encryption Algorithm 3DES-168 • Encapsulation Mode Tunnel • Perfect Forward Secrecy Disabled • Lifetime Measurement Time • Data Lifetime 10000	Select the packet authentication algorithm to use. Select the ESP encryption algorithm to use. Select the Encapsulation Mode for this SA. Select the use of Perfect Forward Secrecy. Select the lifetime measurement of the IPSec keys. Specify the data lifetime in kilobytes (KB).			
Ithe Lifetime power	specify the time metime in seconds.			
IKE Peer 172.18.124.157 Negotiation Mode Main Digital Certificate None (Use Preshared Keys) Certificate Transmission Certificate Transmission Itentity certificate only IKE Proposal IKE-3DES-MD5 Apply Cancel	Specify the IKE Peer for a LAN-to-LAN IPSec connection. Select the IKE Negotiation mode to use. Select the Digital Certificate to use. Choose how to send the digital certificate to the IKE peer. Select the IKE Proposal to use as IKE initiator.			

<u>Checkpoint NG の設定</u>

設定するVPN設定に関連するポリシーを作成するために、Checkpoint NGでネットワークオブジェクトとルールが定義されます。このポリシーは、Checkpoint NG Policy Editorとともにインストールされ、設定のCheckpoint NG側を完了します。

 対象トラフィックを暗号化するCheckpoint NGネットワークとVPNコンセントレータネット 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。オブジェクトを作成するには、 [Manage] > [Network Objects]を選択し、[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 (Checkpoint NGの内部 ネットワーク)およびCONC_INSIDE (VPNコンセントレータ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設定を示しています。

2	etwork Prope	rties - CP_in	side		X
	General NAT	1			
	<u>N</u> ame:	CP_inside			
	IP <u>A</u> ddress	10.32.0.0			
	Net <u>M</u> ask:	255.255.128	3.0		
	<u>C</u> omment:	CPINSIDE			
	Co <u>l</u> or:		·		
	Broadcas	t address:		7	
	• Includ	ed 🤇	Not included		
		OK	Cancel	Help	

Network Prope	ties - CONC_INSIDE	×
General NAT]	
<u>N</u> ame:	CONC_INSIDE	
IP <u>A</u> ddress:	192.168.10.0	
Net <u>M</u> ask:	255.255.255.0	
<u>C</u> omment:	Concentrator network	
Co <u>l</u> or:		
● Broadcas	t address: ed <u>O</u> N <u>o</u> t included	
	OK Cancel Help	

2. VPNデバイス、Checkpoint NG、およびVPNコンセントレータのワークステーションオブジ ェクトを作成するには、[Manage] > [Network Objects]に移動し、[New] > [Workstation]を選 択します。注:初期Checkpoint NGセットアップ時に作成されたCheckpoint 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(Checkpoint NG)およびCISCO_CONC (VPN 3000コンセントレータ)と呼ばれるオ ブジェクトのセットアップを示しています。

Workstation Properties - c	iscocp	×
Workstation Properties - c	iscocp General Name: Ciscocp IP Address: 172.18.124.157 Genment: Checkpoint External IP Color:	×
	Type: C Host C Gateway Check Point Products ✓ Check Epint products installed: Version NG ✓ Get Version ✓VPN-1 & FireWall-1 ✓FloodGate-1 Policy Server ✓ Primary Management Station	
	Object Management Image: Managed by this Management Server (Internal) Image: Managed by another Management Server (External) Secure Internal Communication Image: Description of the transformation Image: Description of the transformation <td< td=""><td></td></td<>	
	OK Cancel He	alp

w	orkstation Properties -	CISCO_CONC	×
	General	General	
	NAT	Name: CISCO_CONC	
		IP Address: 172.18.124.131 Get address	
		Comment: VPN Concentrator	
		Color:	
		Type: C <u>H</u> ost CGate <u>w</u> ay	
		Check Point Products	
		Check Point products installed: Version NG Cet Version	
		VPN-1 & FireWall-1 FloodGate-1 Policy Server Management Station	
		Object Management	
		C Managed by this Management Server (Internal)	
		C Managed by another Management Server (External)	
		Interoperable ⊻PN Device	_
		OK Cancel Help	

[Manage] > [Network Objects] > [Edit]に移動して、Checkpoint 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。[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。この例では、CP_insideはCheckpoint NGの内部ネットワークです。

General	Topology			
NAT	<u>G</u> et Interfaces			
- VPN	Name	IP Address	Network Mask	IP Addresses behind
- Authentication	E100B0	10.32.50.50	255.255.128.0	CP_inside
- Advanced	E100B1	172.18.124.157	255.255.255.0	External
	•			
	<u>A</u> dd	Edit	<u>R</u> emove	Show
	VPN Domain — • All IP Address information.	shind Gateway ses <u>b</u> ehind Gateway b	ased on Topology	Show
	C <u>M</u> anually Def	ined	<u>-</u>	Sho <u>w</u>
	Exportable fo	r SecuRemote		

 Interface Properties]ウィンドウで、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。次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、CP_insideインターフェイスの背後にある IPアドレスを指定します。

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

6. Checkpoint 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 -	ciscocp			×
General Topology NAT VPN Authentication Management € Advanced	VPN Encryption scheme V V VZ V VZ Edt	esset defa	ult <u>I</u> KE properties	
	Nickname ↓	DN dd	Certificate Authority	
		0	IK Cancel	Help

7. VPNコンセントレータのプロパティと一致するようにIKEプロパティを設定します。この例 では、3DESの暗号化オプション**とMD5のハッシング**オプションを選択**します**。

IKE Properties	×
General	
Support key exchange encryption w	ith: – – Support data integrity with: –––
DES A	
Support authentication methods:	
✓ Pre-Shared Secret	Edit <u>S</u> ecrets
Public <u>K</u> ey Signatures	Specify
□ ⊻PN-1 & FireWall-1 authenticat	ion for SecuRemote (Hybrid Mode)
	<u>A</u> dvanced
	ncel Help

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、VPNコンセントレータの事前共有キーと互換性のある事前共有キーを設定します。[Edit]をク**リックし**て、次に[Set]、[OK]の順にクリックします。

Shar	ed Secret				×
\$	Shared Secrets List:				1
	Peer Name CISCO_CONC	Shared S	iecret	<u>E</u> dit	
				<u>R</u> emove	
	Enter secret: cisc	ortprules	Set		
	OK	Car	ncel	<u>H</u> elp	

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。終了したら、「OK」、「OK」の順にクリックします

Advanced IKE properties			×
Use <u>U</u> DP encapsulation	UDP VPN1_IPS	SEC_encapsi 🔻	 [
Support Diffie-Hellman groups —			
	Group 1 (76	8 bit) 124 bit)	
	Group 5 (15	i36 bit)	
Rekeying Parameters	1		
Renegotiate IKE security asso	ociations	1440 🕂	Minutes
Renegotiate IPSEC Security a	associations every	3600 🕂	Seconds
🔲 Renegotiate IPSEC Secur	rity associations eve	ery 50000 🚊	KBytes
Misc Support IP <u>c</u> ompression fo Support <u>agg</u> resive mode Support key exchange for	or SecureClient r <u>s</u> ubnets		
ОК	Cancel	<u>H</u> elp	

10. [Manage] > [Network Objects] > [Edit]に移動し、VPNコンセントレータの[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。この例では、CONC_INSIDE(VPNコンセントレータ 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 - C	ISCO_CONC				×
General Topology	Topology Get Interfaces	1			
- VPN	Name		Network Mask		
Advanced	Add Add Show all IPs be VPN Domain All IP Address information. Manually Defin Exportable for	Edt <u>Edt</u> hind Gateway es <u>b</u> ehind Gateway b ned <u>+ CONC_INS</u> SecuRemote	Bemove	how Show	
			OK Ca	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 -	CISCO_CONC	×
General Topology NAT Advanced	Incruption schemes Image: Im	
	OK Cancel Help	

12. VPNコンセントレータの現在の設定を反映するようにIKEプロパティを設定します。この例 では、3DESの暗号化オプション**とMD5のハッシング**オプションを設**定します**。

IKE Properties	×
General	
Support key exchange encryption w	with: Support data integrity with:
CAST	
Support authentication methods: —	
Pre-Shared Secret	Edit <u>S</u> ecrets
Public <u>K</u> ey Signatures	Matching Criteria
□ VPN-1 & FireWall-1 authentical	tion for SecuRemote (Hybrid Mode)
	<u>A</u> dvanced
OK Ca	ncel Help

13. [Pre-Shared Secrets]の認証オプション**を選択し**て、[**Edit Secrets**]をクリックして事前共有 キーを設定します。[Edit]をク**リックし**て、次に[**Set**]、[**OK**]の順にクリックします。

Sha	red Secret		×
Г	- Shared Secrets List: —		
	Peer Name	Shared Secret	
	ciscocp	****	<u>E</u> dit
			Bemove
	Enter secret: ciscor	tprules Set	
	OK	Cancel	<u>H</u> elp

14. 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。IKEプ ロパティに適切な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。終了したら、「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) CBR	
	Group 5 (1536	s bit)	
Bekeuing Parameters	1		
Reneratiate IKE security associat	ions	1440	Minutes
Developitate IDCEC Convictores	-:	3600	Seconds
Renegotiate IPSEC Security asso	ciations every		VD -
I Renegotiate IPSEL Security a	issociations every		KBytes
Misc			
Support IP compression for Se	ecureClient		
Support aggresive mode	mata		
I ■ Support Key exchange for <u>s</u> uc	nets		
OK C	ancel	<u>H</u> elp	

15. [**Rules**] > [Add Rules] > [Top]を選択し、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、送信元がCP_inside(Checkpoint NGの内部ネットワーク)、宛先が CONC_INSIDE(VPNコンセントレータの内部ネットワーク)の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]を右クリックレ [Edit Properties]を選択します。

Actionj ビフションを追		んり、[ACL	いこともつい	$\gamma \gamma 0$	[⊏ait Prope	iles」を医外	しまり。
CISCOCP - Check Point Policy Editor -	Standar	d					_OX
File Edit View Manage Rules Policy	Topology	Search Window H	ielp				
■ 0 苯铅酯 疊趣演	#	•	- <u>-</u>	54 🗄 🕹 📩			
1 📬 📰 💷 🌮 🗐 💱 🗛 🖉	190	2 🖸 💊 🍈	•				
\$ € 4 0 5 8 0 %	EE Sec	unity - Standard 📳	Address Translation - Sta	ndard 💭 QoS - S	itandard 🛅 Desktop S	iecurity - Standard	
Vetwork Objects	N0.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL
CISCO_CONC	1	부 CP_inside 부 CONC_INSIDE	부 CONC_INSIDE 부 CP_inside	* Any	Edit proper	ties	Galeway:
	2	+ CP_inside	* Any	* Any	G at Edit Encryp	ton Rom	Gateway:
- GP_inside - Gg Domain					💮 accept	12000	
OSE Device					(e) drop		
Group					C Liner Auff		
-W Logical Server					Client Aut	h	
Gateway Ouster	1				🔁 Session /	Auth	•
Dynamic Object	Nan	10	IP	Comment	Encrypt		
	[] CIS	CO_CONC	172.18.1	24.131 VPN Cond	centrator 🙆 Client End	avist	
	🔓 ciso	ocp	172.18.1	24.157 Checkpoi	A Cuery Colu	mn	
					Clear Quer	Y	

16. IKEを選択し、Editをクリックします。

Encryption	n Properties			×
General				
Encr C	yption <u>s</u> chemes defined	:		
	<u>E</u> dit			
	OK	Cancel	Help]

17. IKE Propertiesウィンドウで、VPN Concentrator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)に設定します 。暗号化アルゴリズムを3DESに設定します。[Data Integrity]を[MD5]に設定します。 [Allowed Peer Gateway]をVPNコンセントレータ(CISCO_CONC)と一致するように設定し ます。設定を終えたら 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>C</u> ompression method:	None
Allowed Peer Gateway:	
Use Perfect Forward Secrecy	
Use DH <u>G</u> roup:	Group 1 (768 bit)
Perform IP <u>P</u> ool NAT	
OK Ca	ncel Help

18. Checkpoint NGを設定したら、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				1	
File Edit View Manage Rules	Policy Topology Search Window	Help				
	Venify Instal Uninstall View Access Lists	ddress Translation - St	♥ 📩 🎎 k? andard 🔐 Qo5 - :	Standard 🛅 Desktop	Security - Standard	
Vetwork Objects	Install Users Database	DESTINATION	SERVICE	ACTION	TRACK	INSTALL OF
CISCO_CONC	Management High Availability	부 CONC_INSIDE 부 CP_Inside	* Απγ	C Encrypt	E Log	Gateways
CONC_INSIDE	2 ++ CP_inside	🗙 Any	🗙 Αειγ	😗 accept	Log	C Oateways
CP_inside CP_inside OSE Device Device Embedded Device Group Ugical Server Udical Server Udical Server						
-E Gateway Cluster						<u> </u>
Dynamic Object	Name	IP	Commen	Ł		
		172.18.1 172.18.1	24.131 VPN Con 24.157 Checkpo	centrator int External IP		

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。



ーのインストールが完了したことがインストールウィンドウに表示されたら、[閉じる <u>(Close)]</u>をクリックして手順を完了します。

Install Policy	×
Standard.W: Security Policy Script generated into Standard.pf Standard: Compiled OK.	4
Installing VPN-1/FireWall-1 policy On: ciscocp	
VPN-1/FireWall-1 policy installed successfully on ciscocp	
VPN-1/FireWall-1 policy Installation for all modules was successful	
	-
Close	

確認

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。

ネットワーク通信の確認

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には、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にpingを開始できます。この設定では、Checkpoint NG側 (10.32.50.51)からVPNコンセントレータネットワーク(192.168.10.2)にpingが送信されました。

```
C:\WINNT\System32\cmd.exe
```

C:\>

C:\> C:\> C:\> C:\> C:\> C:\> C:\>ping 192.168.10.2 Pinging 192.168.10.2 with 32 bytes of data: Reply from 192.168.10.2: bytes=32 time=10ms TTL=253 Reply from 192.168.10.2: bytes=32 time=10ms TTL=253 Reply from 192.168.10.2: bytes=32 time<10ms TTL=253 Reply from 192.168.10.2: bytes=32 time<10ms TTL=253 Ping statistics for 192.168.10.2: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = Oms, Maximum = 10ms, Average = 5ms C:\> C:\> C:\> C:\>

<u>チェックポイントNGのトンネルステータスの表示</u>

トンネルのステータスを表示するには、Policy Editorに移動し、**Window > System Status**の順に 選択します。

CISCOCP - Check Point System Status											
Ele Yiew Modules Products Tools Window Help											
) 2 🗉 🖂 🔲 🔌 💷 🇞 💷 🗳 😤	54										
Modules IP Address	VPN-1 Details										
	Status:	ок									
E-Ciscocp 172.18.124.157	Packets										
FireWal-1	Encrypted:	19									
FloodGate-1	Decrypted:	18									
	Errors										
SVN Foundation	Encryption errors:	0									
	Decryption errors:	0									
	IKE events errors:	3									
	Hardware										
	HW Vendor Name:	none									
	HW Status:	none									
<u></u>	1										
For Help, press F1			Last updated:09:34:14 PM								

<u>VPNコンセントレータのトンネルステータスの表示</u>

VPNコンセントレータのトンネルステータスを確認するには、[Administration] > [Administer Sessions]の順に選択します。

dministration Adm	inister Sessions				1	Vednes	iday, 11 Sept	ember 2002 20-37:0 Reset 🅜 Refresh	
his screen shows st aformation on a sess onnection to a sessi	atistics for sessions. ion, click on that sess on, click Ping .	To refresh the statis sion's name. To log	tics, click Refre out a session, cl	sh. Sel ick Log	ect a Group out in the tal	to filter ble belo	the sessions w. To test t	s. For more he network	
roupAll .ogout All: <u>PPTP U</u> Session Summa	ser L2TP User IPS	ec User <u>L2TP/IPS</u> e	ec User IPSec/U	IDP Use	er IPSec/TC	<u>P User</u>	IPSec LAN	I-to-LAN	
Active LAN-to- LAN Sessions Access Sessions Active Management Sessions Sessions Sessions Sessions Sessions Sessions Active Sessions Sessio									
Active LAN-to- LAN Sessions	Active Remote Access Sessions	Management Sessions	Total Active Sessions	Peak (Se	Concurrent essions	Con Sessi	current ons Limit	Total Cumulative Sessions	
Active LAN-to- LAN Sessions	Active Remote Access Sessions	Management Sessions 3	Total Active Sessions 4	Peak (Se	Concurrent essions 4	Con Sessi	ons Limit	Total Cumulative Sessions 17	
Active LAN-to- LAN Sessions 1 LAN-to-LAN S	Active Remote Access Sessions 0 essions	Management Sessions 3	Total Active Sessions	Peak S	Concurrent essions 4 [Remote Ac	Con Sessi	ons Limit 1500 ssions Man	Total Cumulative Sessions 17 agement Sessions]	
Active LAN-to- LAN Sessions 1 LAN-to-LAN S Connection Nan	Active Remote Access Sessions 0 essions ne IP Address	Management Sessions 3 Protoco	Total Active Sessions 4 Encr	Peak S	Concurrent essions 4 [<u>Remote Acc</u> Login T	Con Sessi Cess Se	ssions Man	Total Cumulative Sessions 17 agement Sessions] Actions	

[LAN-to-LAN Sessions]で、作成されたSAの詳細と送受信されたパケットの数を表示するチェッ クポイントの接続名を選択します。

Connection Name	IP Add	fress	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx			
Checkpoint	172.18.12	4.157	IPSec/LAN-to-LAN	3DES-168	Sep 11 20:36:03	0:01:55	256	25			
	Session ID	1	IK	E Session	Encryption Algorit	hum 3DES-1	68				
	Sossion TD	1	IK	E Session	Encryption Algorit	hm 3DES-1	68				
Hashing	Algorithm	MD5		1	Diffie-Hellman Group Group 2 (1024-bit)						
Authentication Mode Pre-Shared Keys				IKE Negotiation Mode Main							
Rekey Tin	e Interval	86400	seconds								
			IPS	ec Session							
:	Session ID	2			Remote Addr	ess 10.32.0.	0/0.0.127.25	55			
Local Address 192.168			8.10.0/0.0.0.255		Encryption Algorit	hm 3DES-1	a 3DES-168				
Hashing	Algorithm	MD5			EP 1	P 1					
Encapsulation Mode Tunnel					Rekey Time Inter	val 28800 s	econds				
ware up sum						contract procession and a second					

<u>トラブルシュート</u>

ここでは、設定のトラブルシューティングに使用できる情報を示します。

注:トラフィックは、VPNコンセントレータのパブリックIPアドレス(外部インターフェイス)を使用してIPSecトンネルを介してPATすることはできません。 そうしないと、トンネルに障害が発生します。したがって、PATに使用されるIPアドレスは、外部インターフェイスに設定されているアドレス以外のアドレスである必要があります。

<u>ネットワーク集約</u>

複数の隣接する内部ネットワークがチェックポイントの暗号化ドメインに設定されている場合、 デバイスは対象トラフィックに関してネットワークを自動的に集約できます。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、これらのネットワークを10.0.0.0 /23に集約できます。

<u>チェックポイントNG のデバッグ</u>

ログを表示するには、[Window] > [Log Viewer]を選択します。

Ta CTSCOCP - Check Point Log Viewer - [fw.log]												×			
Ele	Ele Mode Edit Selection Yew Iools Window Help												1.1		
6	(# 🕼 Log 🔹 👁 🗛 🕈 🛓 💕 🖩 및 😓 📑 🚟 🗟 🗞 🔡 및 🍮 🕘 👔														
	Date	Time	Product	1.1.1	Inter.	Orig	Туре	Action	Source	Destinati	Pr., Rule	S_Port	SrcKeyID	DstKeyID	×
1	13Aug2002	21:32:	VPN-1	& FireN.	💽 dae	ciscocp	🔲 log	0- key instali	ciscoop	CISCO_CONC					
2	13Aug2002	21:32:	VPN-1	& FireVV.	🕒 dee	ciscocp	🔲 log	Over key install	ciscocp	CISCO_CONC			0x5879f30d	0xtt351129	
4															- 1

VPN コンセントレータのデバッグ

VPNコンセントレータでデバッグを有効にするには、[Configuration] > [System] > [Events] > [Classes]に移動します。重大度を1 ~ 13に設定するには、AUTH、AUTHDBG、IKE、IKEDBG、 IPSEC、およびIPSECDBGを有効にします。デバッグを表示するには、[Monitoring] > [Filterable Event Log]を選択します。

1 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=506 172.18.124.157 RECEIVED Message (msgid=0) with payloads : HDR + SA (1) + VENDOR (13) + NONE (0) ... total length : 128

3 09/11/2002 20:36:03.610 SEV=9 IKEDBG/0 RPT=507 172.18.124.157 processing SA payload

4 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=508 Proposal # 1, Transform # 1, Type ISAKMP, Id IKE Parsing received transform: Phase 1 failure against global IKE proposal # 1: Mismatched attr types for class Auth Method: Rcv'd: Preshared Key Cfg'd: XAUTH with Preshared Key (Initiator authenticated)

10 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=509 Phase 1 failure against global IKE proposal # 2: Mismatched attr types for class DH Group: Rcv'd: Oakley Group 2 Cfg'd: Oakley Group 1

13 09/11/2002 20:36:03.610 SEV=7 IKEDBG/0 RPT=510 172.18.124.157 Oakley proposal is acceptable

14 09/11/2002 20:36:03.610 SEV=9 IKEDBG/47 RPT=9 172.18.124.157 processing VID payload

15 09/11/2002 20:36:03.610 SEV=9 IKEDBG/0 RPT=511 172.18.124.157 processing IKE SA

16 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=512
Proposal # 1, Transform # 1, Type ISAKMP, Id IKE
Parsing received transform:
Phase 1 failure against global IKE proposal # 1:
Mismatched attr types for class Auth Method:
Rcv'd: Preshared Key
Cfg'd: XAUTH with Preshared Key (Initiator authenticated)

22 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=513 Phase 1 failure against global IKE proposal # 2: Mismatched attr types for class DH Group: Rcv'd: Oakley Group 2 Cfg'd: Oakley Group 1

25 09/11/2002 20:36:03.610 SEV=7 IKEDBG/28 RPT=9 172.18.124.157 IKE SA Proposal # 1, Transform # 1 acceptable Matches global IKE entry # 3

26 09/11/2002 20:36:03.610 SEV=9 IKEDBG/0 RPT=514 172.18.124.157 constructing ISA_SA for isakmp

27 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=515 172.18.124.157 SENDING Message (msgid=0) with payloads : HDR + SA (1) + NONE (0) ... total length : 84

29 09/11/2002 20:36:03.630 SEV=8 IKEDBG/0 RPT=516 172.18.124.157

RECEIVED Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 184 31 09/11/2002 20:36:03.630 SEV=8 IKEDBG/0 RPT=517 172.18.124.157 RECEIVED Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 184 33 09/11/2002 20:36:03.630 SEV=9 IKEDBG/0 RPT=518 172.18.124.157 processing ke payload 34 09/11/2002 20:36:03.630 SEV=9 IKEDBG/0 RPT=519 172.18.124.157 processing ISA_KE 35 09/11/2002 20:36:03.630 SEV=9 IKEDBG/1 RPT=91 172.18.124.157 processing nonce payload 36 09/11/2002 20:36:03.660 SEV=9 IKEDBG/0 RPT=520 172.18.124.157 constructing ke payload 37 09/11/2002 20:36:03.660 SEV=9 IKEDBG/1 RPT=92 172.18.124.157 constructing nonce payload 38 09/11/2002 20:36:03.660 SEV=9 IKEDBG/46 RPT=37 172.18.124.157 constructing Cisco Unity VID payload 39 09/11/2002 20:36:03.660 SEV=9 IKEDBG/46 RPT=38 172.18.124.157 constructing xauth V6 VID payload 40 09/11/2002 20:36:03.660 SEV=9 IKEDBG/48 RPT=19 172.18.124.157 Send TOS VID 41 09/11/2002 20:36:03.660 SEV=9 IKEDBG/38 RPT=10 172.18.124.157 Constructing VPN 3000 spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 2000001) 43 09/11/2002 20:36:03.660 SEV=9 IKEDBG/46 RPT=39 172.18.124.157 constructing VID payload 44 09/11/2002 20:36:03.660 SEV=9 IKEDBG/48 RPT=20 172.18.124.157 Send Altiga GW VID 45 09/11/2002 20:36:03.660 SEV=9 IKEDBG/0 RPT=521 172.18.124.157 Generating keys for Responder... 46 09/11/2002 20:36:03.670 SEV=8 IKEDBG/0 RPT=522 172.18.124.157 SENDING Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) ... total length : 256 48 09/11/2002 20:36:03.690 SEV=8 IKEDBG/0 RPT=523 172.18.124.157 RECEIVED Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + NONE (0) ... total length : 60 50 09/11/2002 20:36:03.690 SEV=9 IKEDBG/1 RPT=93 172.18.124.157 Group [172.18.124.157] Processing ID 51 09/11/2002 20:36:03.690 SEV=9 IKEDBG/0 RPT=524 172.18.124.157 Group [172.18.124.157] processing hash 52 09/11/2002 20:36:03.690 SEV=9 IKEDBG/0 RPT=525 172.18.124.157 Group [172.18.124.157] computing hash

53 09/11/2002 20:36:03.690 SEV=9 IKEDBG/23 RPT=10 172.18.124.157 Group [172.18.124.157] Starting group lookup for peer 172.18.124.157 54 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/1 RPT=10 AUTH_Open() returns 9 55 09/11/2002 20:36:03.690 SEV=7 AUTH/12 RPT=10 Authentication session opened: handle = 9 56 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/3 RPT=10 AUTH_PutAttrTable(9, 748174) 57 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/6 RPT=10 AUTH_GroupAuthenticate(9, 2f1b19c, 49c648) 58 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/59 RPT=10 AUTH_BindServer(51a6b48, 0, 0) 59 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/69 RPT=10 Auth Server e054d4 has been bound to ACB 51a6b48, sessions = 1 60 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/65 RPT=10 AUTH_CreateTimer(51a6b48, 0, 0) 61 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/72 RPT=10 Reply timer created: handle = 4B0018 62 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/61 RPT=10 AUTH_BuildMsg(51a6b48, 0, 0) 63 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/64 RPT=10 AUTH_StartTimer(51a6b48, 0, 0) 64 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/73 RPT=10 Reply timer started: handle = 4B0018, timestamp = 1163319, timeout = 3000065 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/62 RPT=10 AUTH_SndRequest(51a6b48, 0, 0) 66 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/50 RPT=19 IntDB_Decode(3825300, 156) 67 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/47 RPT=19 IntDB_Xmt(51a6b48) 68 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/71 RPT=10 $xmit_cnt = 1$ 69 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/47 RPT=20 IntDB_Xmt(51a6b48) 70 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/49 RPT=10 IntDB_Match(51a6b48, 3eb7ab0) 71 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/63 RPT=10 AUTH_RcvReply(51a6b48, 0, 0) 72 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/50 RPT=20 IntDB_Decode(3eb7ab0, 298) 73 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/48 RPT=10 IntDB_Rcv(51a6b48)

74 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/66 RPT=10 AUTH_DeleteTimer(51a6b48, 0, 0) 75 09/11/2002 20:36:03.790 SEV=9 AUTHDBG/74 RPT=10 Reply timer stopped: handle = 4B0018, timestamp = 1163329 76 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/58 RPT=10 AUTH_Callback(51a6b48, 0, 0) 77 09/11/2002 20:36:03.790 SEV=6 AUTH/41 RPT=10 172.18.124.157 Authentication successful: handle = 9, server = Internal, group = 172.18.124.15778 09/11/2002 20:36:03.790 SEV=7 IKEDBG/0 RPT=526 172.18.124.157 Group [172.18.124.157] Found Phase 1 Group (172.18.124.157) 79 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/4 RPT=10 AUTH_GetAttrTable(9, 748420) 80 09/11/2002 20:36:03.790 SEV=7 IKEDBG/14 RPT=10 172.18.124.157 Group [172.18.124.157] Authentication configured for Internal 81 09/11/2002 20:36:03.790 SEV=9 IKEDBG/19 RPT=19 172.18.124.157 Group [172.18.124.157] IKEGetUserAttributes: IP Compression = disabled 82 09/11/2002 20:36:03.790 SEV=9 IKEDBG/19 RPT=20 172.18.124.157 Group [172.18.124.157] IKEGetUserAttributes: Split Tunneling Policy = Disabled 83 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/2 RPT=10 AUTH_Close(9) 84 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=94 172.18.124.157 Group [172.18.124.157] constructing ID 85 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=527 Group [172.18.124.157] construct hash payload 86 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=528 172.18.124.157 Group [172.18.124.157] computing hash 87 09/11/2002 20:36:03.790 SEV=9 IKEDBG/46 RPT=40 172.18.124.157 Group [172.18.124.157] constructing dpd vid payload 88 09/11/2002 20:36:03.790 SEV=8 IKEDBG/0 RPT=529 172.18.124.157 SENDING Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) ... total length : 80 90 09/11/2002 20:36:03.790 SEV=4 IKE/119 RPT=10 172.18.124.157 Group [172.18.124.157] PHASE 1 COMPLETED 91 09/11/2002 20:36:03.790 SEV=6 IKE/121 RPT=10 172.18.124.157 Keep-alive type for this connection: None

92 09/11/2002 20:36:03.790 SEV=6 IKE/122 RPT=10 172.18.124.157

Keep-alives configured on but peer does not support keep-alives (type = None) 93 09/11/2002 20:36:03.790 SEV=7 IKEDBG/0 RPT=530 172.18.124.157 Group [172.18.124.157] Starting phase 1 rekey timer: 64800000 (ms) 94 09/11/2002 20:36:03.790 SEV=4 AUTH/22 RPT=16 User 172.18.124.157 connected 95 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/60 RPT=10 AUTH_UnbindServer(51a6b48, 0, 0) 96 09/11/2002 20:36:03.790 SEV=9 AUTHDBG/70 RPT=10 Auth Server e054d4 has been unbound from ACB 51a6b48, sessions = 0 97 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/10 RPT=10 AUTH_Int_FreeAuthCB(51a6b48) 98 09/11/2002 20:36:03.790 SEV=7 AUTH/13 RPT=10 Authentication session closed: handle = 9 99 09/11/2002 20:36:03.790 SEV=8 IKEDBG/0 RPT=531 172.18.124.157 RECEIVED Message (msgid=54796f76) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) ... total length : 156 102 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=532 172.18.124.157 Group [172.18.124.157] processing hash 103 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=533 172.18.124.157 Group [172.18.124.157] processing SA payload 104 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=95 172.18.124.157 Group [172.18.124.157] processing nonce payload 105 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=96 172.18.124.157 Group [172.18.124.157] Processing ID 106 09/11/2002 20:36:03.790 SEV=5 IKE/35 RPT=6 172.18.124.157 Group [172.18.124.157] Received remote IP Proxy Subnet data in ID Payload: Address 10.32.0.0, Mask 255.255.128.0, Protocol 0, Port 0 109 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=97 172.18.124.157 Group [172.18.124.157] Processing ID 110 09/11/2002 20:36:03.790 SEV=5 IKE/34 RPT=6 172.18.124.157 Group [172.18.124.157] Received local IP Proxy Subnet data in ID Payload: Address 192.168.10.0, Mask 255.255.255.0, Protocol 0, Port 0 113 09/11/2002 20:36:03.790 SEV=8 IKEDBG/0 RPT=534 QM IsRekeyed old sa not found by addr 114 09/11/2002 20:36:03.790 SEV=5 IKE/66 RPT=8 172.18.124.157 Group [172.18.124.157]

IKE Remote Peer configured for SA: L2L: Checkpoint

115 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=535 172.18.124.157 Group [172.18.124.157] processing IPSEC SA

116 09/11/2002 20:36:03.790 SEV=7 IKEDBG/27 RPT=8 172.18.124.157 Group [172.18.124.157] IPSec SA Proposal # 1, Transform # 1 acceptable

117 09/11/2002 20:36:03.790 SEV=7 IKEDBG/0 RPT=536 172.18.124.157 Group [172.18.124.157] IKE: requesting SPI!

118 09/11/2002 20:36:03.790 SEV=9 IPSECDBG/6 RPT=39 IPSEC key message parse - msgtype 6, len 200, vers 1, pid 00000000, seq 10, err 0, type 2, mode 0, state 32, label 0, pad 0, spi 00000000, encrKeyLen 0, hashKeyLen 0, ivlen 0, alg 0, hmacAlg 0, lifetype 0, lifetime1 17248580, lifetime2 0, dsId 300

122 09/11/2002 20:36:03.790 SEV=9 IPSECDBG/1 RPT=139 Processing KEY_GETSPI msg!

123 09/11/2002 20:36:03.790 SEV=7 IPSECDBG/13 RPT=10 Reserved SPI 305440147

124 09/11/2002 20:36:03.790 SEV=8 IKEDBG/6 RPT=10 IKE got SPI from key engine: SPI = 0x1234a593

125 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=537 172.18.124.157 Group [172.18.124.157] oakley constucting quick mode

126 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=538 172.18.124.157 Group [172.18.124.157] constructing blank hash

127 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=539 172.18.124.157 Group [172.18.124.157] constructing ISA_SA for ipsec

128 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=98 172.18.124.157 Group [172.18.124.157] constructing ipsec nonce payload

129 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=99 172.18.124.157 Group [172.18.124.157] constructing proxy ID

130 09/11/2002 20:36:03.800 SEV=7 IKEDBG/0 RPT=540 172.18.124.157 Group [172.18.124.157] Transmitting Proxy Id: Remote subnet: 10.32.0.0 Mask 255.255.128.0 Protocol 0 Port 0 Local subnet: 192.168.10.0 mask 255.255.255.0 Protocol 0 Port 0

134 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=541 172.18.124.157 Group [172.18.124.157] constructing qm hash

135 09/11/2002 20:36:03.800 SEV=8 IKEDBG/0 RPT=542 172.18.124.157 SENDING Message (msgid=54796f76) with payloads : HDR + HASH (8) + SA (1) ... total length : 152

137 09/11/2002 20:36:03.800 SEV=8 IKEDBG/0 RPT=543 172.18.124.157 RECEIVED Message (msgid=54796f76) with payloads : HDR + HASH (8) + NONE (0) ... total length : 48

139 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=544 172.18.124.157 Group [172.18.124.157] processing hash 140 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=545 172.18.124.157 Group [172.18.124.157] loading all IPSEC SAs 141 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=100 172.18.124.157 Group [172.18.124.157] Generating Quick Mode Key! 142 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=101 172.18.124.157 Group [172.18.124.157] Generating Quick Mode Key! 143 09/11/2002 20:36:03.800 SEV=7 IKEDBG/0 RPT=546 172.18.124.157 Group [172.18.124.157] Loading subnet: Dst: 192.168.10.0 mask: 255.255.255.0 Src: 10.32.0.0 mask: 255.255.128.0 146 09/11/2002 20:36:03.800 SEV=4 IKE/49 RPT=7 172.18.124.157 Group [172.18.124.157] Security negotiation complete for LAN-to-LAN Group (172.18.124.157) Responder, Inbound SPI = 0x1234a593, Outbound SPI = 0x0df37959 149 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/6 RPT=40 IPSEC key message parse - msgtype 1, len 606, vers 1, pid 0000000, seq 0, err 0, type 2, mode 1, state 64, label 0, pad 0, spi 0df37959, encrKeyLen 24, hashKeyLen 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 17248580, lifetime2 0, dsId 0 153 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/1 RPT=140 Processing KEY_ADD msg! 154 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/1 RPT=141 key_msghdr2secassoc(): Enter 155 09/11/2002 20:36:03.800 SEV=7 IPSECDBG/1 RPT=142 No USER filter configured 156 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/1 RPT=143 KeyProcessAdd: Enter 157 09/11/2002 20:36:03.800 SEV=8 IPSECDBG/1 RPT=144 KeyProcessAdd: Adding outbound SA

158 09/11/2002 20:36:03.800 SEV=8 IPSECDBG/1 RPT=145 KeyProcessAdd: src 192.168.10.0 mask 0.0.0.255, dst 10.32.0.0 mask 0.0.127.255

159 09/11/2002 20:36:03.810 SEV=8 IPSECDBG/1 RPT=146 KeyProcessAdd: FilterIpsecAddIkeSa success

160 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/6 RPT=41 IPSEC key message parse - msgtype 3, len 327, vers 1, pid 00000000, seq 0, err 0, type 2, mode 1, state 32, label 0, pad 0, spi 1234a593, encrKeyLen 24, hashKeyLen 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 17248580, lifetime2 0, dsId 0

164 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=147 Processing KEY_UPDATE msg!

165 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=148 Update inbound SA addresses

166 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=149
key_msghdr2secassoc(): Enter

167 09/11/2002 20:36:03.810 SEV=7 IPSECDBG/1 RPT=150 No USER filter configured

168 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=151 KeyProcessUpdate: Enter

169 09/11/2002 20:36:03.810 SEV=8 IPSECDBG/1 RPT=152 KeyProcessUpdate: success

170 09/11/2002 20:36:03.810 SEV=8 IKEDBG/7 RPT=7 IKE got a KEY_ADD msg for SA: SPI = 0x0df37959

171 09/11/2002 20:36:03.810 SEV=8 IKEDBG/0 RPT=547 pitcher: rcv KEY_UPDATE, spi 0x1234a593

172 09/11/2002 20:36:03.810 SEV=4 IKE/120 RPT=7 172.18.124.157 Group [172.18.124.157] PHASE 2 COMPLETED (msgid=54796f76)

関連情報

- Cisco VPN 3000 シリーズ コンセントレータに関するサポート ページ
- <u>Cisco VPN 3000 シリーズ クライアントに関するサポート ページ</u>
- IPSec に関するサポート ページ
- ・<u>テクニカルサポート Cisco Systems</u>