Cisco RV320ギガビットデュアルWAN VPNルー タとCisco 500シリーズサービス統合型アダプタ 間のサイト間VPNトンネルの設定

目的

バーチャルプライベートネットワーク(VPN)は、リモートネットワークをメインのプライベ ートネットワークに接続するために広く使用されているテクノロジーとして存在し、パブリ ックライン上で暗号化されたチャネルの形でプライベートリンクをシミュレートします。 VPNトラフィックを暗号化する2段階のネゴシエーションにより、VPNエンドポイントのみ が復号化を認識できる方法で行われるため、リモートネットワークはセキュリティ上の問題 なく、プライベートのメインネットワークの一部として存在するように接続できます。 この短いガイドでは、Cisco 500シリーズサービス統合型アダプタとCisco RVシリーズルー タの間にサイト間IPsec VPNトンネルを構築するための設計例を示します。

該当するデバイス

- ・ Cisco RVシリーズルータ(RV320)
- ・ Cisco 500シリーズサービス統合型アダプタ(ISA570)

[Software Version]

・ 4.2.2.08 [Cisco RV0xxシリーズVPNルータ]

事前設定

ネットワーク図 次に、サイト間VPNトポロジを示します。



サイト間IPsec VPNトンネルは、リモートオフィスのCisco RVシリーズルータと本社の Cisco 500シリーズISAの間で設定および確立されます。 この設定では、リモートオフィスのLAN 192.168.1.0/24のホストと、本社のLAN 10.10.0/24のホストが、VPNを介して互いに安全に通信できます。

コアコンセプト

ンターネット キー交換(IKE)

Internet Key Exchange (IKE;インターネットキーエクスチェンジ)は、IPsecプロトコル スイートでセキュリティアソシエーション(SA)をセットアップするために使用されるプロト コルです。IKEは、Oakleyプロトコル、Internet Security Association、およびKey Management Protocol(ISAKMP)に基づいて構築され、Diffie-Hellman(DH)キー交換を使用し て共有セッションシークレットを設定し、そこから暗号キーを取得します。

Internet Security Association and Key Management Protocol (ISAKMP)

Internet Security Association and Key Management Protocol(ISAKMP)は、2つのVPNエンド ポイント間でVPNトンネルをネゴシエートするために使用されます。認証、通信、およびキ 一生成の手順を定義し、IKEプロトコルで暗号キーを交換してセキュア接続を確立します。

IPSec (Internet Protocol Security)

IP Security Protocol(IPsec)は、データストリームの各IPパケットを認証および暗号化することによって、IP通信を保護するためのプロトコルスイートです。IPsecには、セッションの開始時にエージェント間で相互認証を確立するためのプロトコルや、セッション中に使用される暗号キーのネゴシエーションも含まれます。IPsecは、ホスト、ゲートウェイ、またはネットワークのペア間のデータフローを保護するために使用できます。

設計のヒント

VPNトポロジ:ポイントツーポイントVPNトポロジとは、メインサイトとリモートサイト

の間にセキュアなIPsecトンネルが設定されていることを意味します。

企業では、多くの場合、マルチサイトトポロジで複数のリモートサイトを必要とし、ハブア ンドスポークVPNトポロジまたはフルメッシュVPNトポロジを実装します。ハブアンドス ポークVPNトポロジとは、リモートサイトが他のリモートサイトと通信する必要がなく、各 リモートサイトはメインサイトとのセキュアなIPsecトンネルのみを確立することを意味し ます。フルメッシュVPNトポロジは、リモートサイトが他のリモートサイトと通信する必要 があることを意味し、各リモートサイトはメインサイトおよびその他すべてのリモートサイ トとのセキュアなIPsecトンネルを確立します。

VPN認証:VPNトンネルの確立時にVPNピアを認証するためにIKEプロトコルが使用されます 。さまざまなIKE認証方式が存在し、事前共有キーが最も便利な方式です。シスコでは、強 力な事前共有キーの適用を推奨しています。

VPN暗号化:VPN経由で転送されるデータの機密性を確保するために、暗号化アルゴリズム を使用してIPパケットのペイロードを暗号化します。DES、3DES、およびAESは、3つの 一般的な暗号化規格です。AESは、DESおよび3DESと比較して最も安全であると考えられ ています。シスコでは、AES-128ビット以上の暗号化(AES-192やAES-256など)を適用す ることを強く推奨しています。ただし、強力な暗号化アルゴリズムでは、ルータからより 多くの処理リソースが必要になります。

ダイナミックWAN IPアドレッシングおよびダイナミックドメインネームサービス(DDNS) :2つのパブリックIPアドレス間でVPNトンネルを確立する必要があります。WANルータが インターネットサービスプロバイダー(ISP)からスタティックIPアドレスを受信する場合、 スタティックなパブリックIPアドレスを使用してVPNトンネルを直接実装できます。しかし 、ほとんどの小規模企業は、DSLやケーブルなどのコスト効率の高いブロードバンドインタ ーネットサービスを使用し、ISPからダイナミックIPアドレスを受信しています。このよう な場合、ダイナミックドメインネームサービス(DDNS)を使用して、ダイナミックIPアドレ スを完全修飾ドメイン名(FQDN)にマッピングできます。

LAN IPアドレッシング: 各サイトのプライベートLAN IPネットワークアドレスは重複しな いようにしてください。各リモートサイトのデフォルトLAN IPネットワークアドレスは、 常に変更する必要があります。

設定のヒント

設定前チェックリスト

ステップ1:RV320とDSLまたはケーブルモデムの間にイーサネットケーブルを接続し、 ISA570とDSLまたはケーブルモデムの間にイーサネットケーブルを接続します。 ステップ2:RV320をオンにし、内部PC、サーバ、およびその他のIPデバイスをRV320の LANポートに接続します。

ステップ3:ISA570をオンにし、内部PC、サーバ、およびその他のIPデバイスをISA570の LANポートに接続します。

手順4:異なるサブネット上の各サイトでネットワークIPアドレスを設定します。この例で は、リモートオフィスLANは192.168.1.0を使用し、本社LANは10.10.0のを使用しています 。

ステップ5:ローカルPCがそれぞれのルータと、同じLAN上の他のPCに接続できることを 確認します。

WAN接続の特定

ISPがダイナミックIPアドレスまたはスタティックIPアドレスを提供しているかどうかを確認する必要があります。通常、ISPはダイナミックIPアドレスを提供しますが、サイト間 VPNトンネル設定を完了する前に、これを確認する必要があります。

リモートオフィスでのRV320用のサイト間IPsec VPNトンネルの設定

ステップ1:[VPN] > [Gateway-to-Gateway]に移動します(図を参照)

- a.) トンネル名(RemoteOfficeなど)を入力します。
- b.) インターフェイスをWAN1に設定します。
- c.)事前共有キーを使用して、キーイングモードをIKEに設定します。
- d.) [Local IP Address]と[Remote IP Address]を入力します。

次の図は、[RV320 Gigabit Dual WAN Router Gateway to Gateway]ページを示しています。

CISCO RV320 Gig	gabit Dual WAN VPN R	outer
Getting Started System Summary	Gateway to Gateway	
▶ Setup	Add a New Tunnel	
► DHCP	Tunnel No.	2
System Management Port Management	Tunnel Name:	
▶ Firewall	Interface:	WAN1
✓ VPN Summary	Keying Mode:	IKE with Preshared key
Gateway to Gateway Client to Gateway	Enable:	
VPN Passtnrougn PPTP Server	Local Group Setup	
 Certificate Management 	Local Security Gateway Type:	IP Only
► Log ► SSL VPN	IP Address:	0.0.0.0
User Management	Local Security Group Type:	Subnet
Wizard	IP Address:	192.168.1.0
	Subnet Mask:	255.255.255.0
	Remote Group Setup	
	Remote Security Gateway Type:	IP Only
	IP Address 🗸 🗸	
	Remote Security Group Type:	Subnet 🗸
	IP Address:	
© 2013 Cisco Systems, Inc. All Rig	ghts Reserved.	

ステップ2:IPSecトンネル設定の設定(図を参照)

a.) [暗号化]を3DESに設定します。

- b.) [Authentication]を[SHA1]に設定します。
- c.) Perfect Forward Secrecyをチェックします。
- d.) 事前共有キーを設定します(両方のルータで同じにする必要があります)。
- 次に、IPSecセットアップ(フェーズ1および2)を示します。

IPSec Setup		
Phase 1 DH Group:	Group 2 - 1024 bit 🗸	
Phase 1 Encryption :	3DES 🗸	
Phase 1 Authentication:	SHA1 🗸	
Phase 1 SA Lifetime:	600	sec (Range: 120-86400, Default: 28800)
Perfect Forward Secrecy:		
Phase 2 DH Group:	Group 2 - 1024 bit 🗸	
Phase 2 Encryption:	3DES 🗸	
Phase 2 Authentication:	SHA1 🗸	
Phase 2 SA Lifetime:	600	sec (Range: 120-28800, Default: 3600)
Minimum Preshared Key Complexity:	Enable	
Preshared Key:	Aa1234567890!@#\$%^&*()_+	
Preshared Key Strength Meter:		
Advanced +		

注:サイト間IPsec VPNトンネルの両側のIPsecトンネル設定が一致する必要があることに 注意してください。RV320とISA570のIPsecトンネル設定に不一致がある場合、両方のデバ イスが暗号化キーのネゴシエートに失敗し、接続に失敗します。 ステップ3:[Save]をクリックし、設定を完了します。

本社のISA570用サイト間IPsec VPNトンネルの設定

ステップ1:[VPN] > [IKE Policies]に移動します(図を参照)。

a.) 暗号化をESP_3DESに設定します。

b.) ハッシュをSHA1に設定します。

c.) [Authentication] を[Pre-shared Key]に設定します。

d.) [D-H Group]を[Group 2 (1024ビット)]に設定します。

次の図に、IKEポリシーを示します。

Small Business						
cisco ISA500 Series Col	nfiguration Utility	'		and and the second		
Conliguration wizards	IKE Policies					
Status	IKE Policies					
Networking	+ Add X Delete					
Firewall	□ Namo	Encorro	tion	Hach	Authontication	D.H.Group
Security Services			56			group 2
VPN		3055	IKE Dolicy A	dd/Edit	Heln	group_2
▼ VPN Status	11/320	JDEC	IKE POIICY - A	uu/cuit		group_2
IPsec VPN Status			Name:	rv320		
SSL VPN Status			Encryption:	ESP_3DES		
 Site-to-Site IPsoc Policios 			Hach:			
IKE Policies			nasıı.			
Transform Sets			Authenticatio	n: • Pre-shared Key () RSA_SI	G	
IPsec Remote Access			D-H Group:	Group 2 (1024bits) 💌		
 SSL Remote User Access 						
Teleworker VPN Client			Lifetime:	Hour Min Sec (F	Range: 3 minutes to 24 hours)	
L2TP Server						
VPN Passthrough	Save Cancel					
					Caller	
Users						
Device Management						
	_					

ステップ2:[VPN] > [IKE Transform Sets]に移動します(図を参照)

a.) [Integrity] を[ESP_SHA1_HMAC]に設定します。

b.) [Encryption]*を[*ESP_DES]に設定します。

次に、IKEトランスフォームセットを示します。

Small Business cisco ISA500 Series	Configuration Utility		
Configuration Wizards Status Networking Firewall	Transform Sets		
Security Services VPN VPN Status	DefaultTrans rv320	Integrity ESP_SHA1_HMAC ESP_SHA1_HMAC	ESP_AES_256 ESP_3DES
IPsec VPN Status SSL VPN Status ▼ Site-to-Site IPsec Policies IKE Policies Transform Sets IPsec Remote Access ▶ SSL Remote User Access		Transform Set - Add/Edit Name: 17320 ESP Integrity: ESP_MD5_HMAC • E Encryption: ESP_3DES •	Heig ESP_SHA1_HMAC
L2TP Server VPN Passthrough	Save Cancel		OK Cancel

ステップ3:[VPN] > [IPsec Policies] > [Add] > [Basic Settings]に移動します(図を参照)。

- a.) RV320な ど、説明を入力します。
- b.) IPsecポリシーの有効化をオンに設定します。
- c.) [Remote Type] を[Static IP]に設定します。
- d.) リモートア *ドレスを入力*。
- e.) [Authentication Method] を[Pre-Shared Key]に設定します。
- f) WANインタ ーフェイスをWAN1に設定します。
- g.) ローカ ル・ネットワークをDEFAULT_NETWORKに設定します。

h.) リモートネ ットワークをRV320に設定します。 次の図に、IPsecポリシーの基本設定を示します。

Small Business cisco ISA500 Series Co	nfiguration l	Jtility		
Configuration Wizards	IPsec Polic	ies		
Status	Il See l'ond	IDsec Dolicies Add/Edit		Hein
Networking	Enable VPN:	IFSEC FOICIES - Auu/Luit		
Firewall	IPsec Policie	Basic Settings Advanced Setti	ngs VPN Failover	
Security Services	+ Add 🗙	* Description: rv32	0	
VPN	Name	* IPsec Policy Enable: 0	n 🔿 Off	IKE
▼ VPN Status	rv320	* Remote Type: Stat	ic IP 💌	rv320
IPsec VPN Status		Barrada Addasaa		
Site-to-Site		Remote Address: 10.1	10.10.2	
IPsec Policies		* Authentication Method: F 	Pre-Shared Key	
IKE Policies		* Key:	Aa1234567890!@#\$%^&*()	
Transform Sets		0 0	Certificate	
 SSL Remote User Access 		Loca	I Certificate: default 👻	
Teleworker VPN Client		Rem	ote Certificate: default 💌	
L2TP Server		WAN Interface: WAN	N1 🔍	
VPN Passthrough				
	Sava Canad	* Local network:		
	Save Cancer	* Remote network: rv32	10 💌	
				OK Cancel
Users				

ステップ4:[VPN] > [**IPsec Policies] > [Add] > [Advanced Settings]に移動**します(図を参照)。 a.) IKEポリ *シーと IKEトランスフォーム*セットを、手順1と2で作成したセットにそれぞれ設定し ます。

b.) SA- Lifetimeを0時間5分0秒に設定します。

c.) [OK] をクリックします。

次に、IPsecポリシーの詳細設定を示します。

Small Business cisco ISA500 Series Cor	nfiguration L	Jtility					
Configuration Wizards	IPsec Polici	ies					
Status		IDsec Dolicies Add/Edit				Help	
Networking	Enable VPN:	IF SEC FOILES - Add/Edit					
Firewall	IPsec Policie	Basic Settings Advance	d Settings VPN F	allover			
Security Services	🕂 Add 🗙	Windows Networking (Net BIOS) Broadcast:	🔾 On 💿 Off			^	
VPN	Name	Access Control :	Zone	Access Setting			IKE
▼ VPN Status	□ rv320		LAN	Permit Deny			rv320
IPsec VPN Status			WAN	Permit Deny			
SSL VPN Status			DMZ	Permit Deny			
IPsec Policies			GUEST	Permit Deny			
IKE Policies			SSLVPN	Permit Deny			
Transform Sets			VOICE	Permit Deny			
IPsec Remote Access							
SSL Remote User Access		Apply NAT Policies:	O On (Off			
Late Server			_ Selec	t an address object 💌			
VPN Passthrough		I ranslated Local Netwo	ork:	tun uuness objeet –			
vi ivi assunougn		Translated Remote Ne	twork: - Selec	t an address object 💌			
	Save Cancel	IKE Policy:	rv320	IKE Policy Link			
		Transform:	rv320	Transform Link			
		SA-Lifetime:	0 н	our 5 Min 0 Sec	(Range: 3 minutes to 24 h	ours) 🗸	
					O	Cancel	
Users							

ステップ5 : サイト間IPsec VPNトンネルの接続(図を参照) a.) [Enable VPN] *を[*On *]に*設定します。 b.) [接続]ボタ **ンをクリッ**クします。 次の図は、[Connect]ボタンを示しています。

Psec Policies					
Enable VPN: 💿 O	n O Off				
IPsec Policies					
🕂 Add 🗙 Delete	🛞 Refresh				
ers	Local	Remote	IKE	Transform	Configure
.10.10.2	*DEFAULT_NETWORK	rv320	rv320	rv320	/X \\