# 在Cisco RV320 Gigabit Dual WAN VPN路由器和 Cisco 500系列整合服務介面卡之間配置站點到站 點VPN隧道

# 目標

虛擬私有網路(VPN)是一種廣泛使用的技術,用於將遠端網路連線到主私有網路,在公共線路 上模擬以加密通道形式的私有連結。遠端網路可以連線到專用主網路,就像它作為專用主網路 的一部分存在一樣,而不存在安全隱患,這是因為2階段協商會以只有VPN端點知道如何解密 的方式加密VPN流量。

本簡要指南提供在Cisco 500系列整合服務介面卡和Cisco RV系列路由器之間構建站點到站點 IPsec VPN隧道的示例設計。

# 適用裝置

·Cisco RV系列路由器(RV320) ·思科500系列整合多業務介面卡(ISA570)

## 軟體版本

·4.2.2.08 [Cisco RV0xx系列VPN路由器]

# 預配置

網路圖表

下面顯示了站點到站點VPN拓撲。



在遠端辦公室的Cisco RV系列路由器與總部的Cisco 500系列ISA之間配置並建立站點到站點 IPsec VPN隧道。 通過此配置,遠端辦公室的LAN 192.168.1.0/24中的主機和總部的LAN 10.10.10.0/24中的主 機可以通過VPN安全地相互通訊。

### 核心概念

#### 網際網路金鑰交換(IKE)

Internet金鑰交換(IKE)是用於在IPsec協定套件中設定安全關聯(SA)的協定。IKE在Oakley協定、Internet安全關聯和金鑰管理協定(ISAKMP)的基礎上構建,並使用Diffie-Hellman金鑰交換 來設定共用會話金鑰,從會話金鑰中匯出加密金鑰。

#### 網際網路安全性關聯和金鑰管理通訊協定(ISAKMP)

Internet安全關聯和金鑰管理協定(ISAKMP)用於協商兩個VPN端點之間的VPN隧道,它定義了 身份驗證、通訊和金鑰生成過程,並由IKE協定用於交換加密金鑰和建立安全連線。

#### 網際網路通訊協定安全(IPsec)

IP安全通訊協定(IPsec)是一種通訊協定套件,用於透過驗證和加密資料流的每個IP封包來保護 IP通訊。IPsec還包括一些協定,用於在會話開始時代理之間建立相互身份驗證,以及協商會 話期間使用的加密金鑰。 IPsec可用於保護主機、網關或網路之間的資料流。

#### 設計提示

VPN拓撲 — 點對點VPN拓撲意味著在主站點和遠端站點之間配置了一個安全的IPsec隧道。 企業通常需要多站點拓撲中的多個遠端站點,並實施中心輻射型VPN拓撲或全網狀VPN拓撲 。集中星型VPN拓撲意味著遠端站點不需要與其他遠端站點通訊,並且每個遠端站點只與主站 點建立安全的IPsec隧道。全網狀VPN拓撲意味著遠端站點需要與其他遠端站點通訊,並且每 個遠端站點與主站點和所有其他遠端站點建立安全的IPsec隧道。

VPN驗證 — 在建立VPN隧道時,IKE協定用於驗證VPN對等體。存在各種IKE身份驗證方法 ,而預共用金鑰是最方便的方法。思科建議應用強預共用金鑰。

VPN加密 — 為了確保通過VPN傳輸的資料的機密性,使用加密演算法來加密IP資料包的負載 。DES、3DES和AES是三種常見的加密標準。與DES和3DES相比,AES被認為是最安全的 。思科強烈建議應用AES-128位或更高的加密(例如AES-192和AES-256)。 但是,更強的 加密演算法需要路由器提供更多的處理資源。

動態WAN IP編址和動態域名服務(DDNS) — 需要在兩個公共IP地址之間建立VPN隧道。如果 WAN路由器收到來自網際網路服務提供商(ISP)的靜態IP地址,則可直接使用靜態公共IP地址 來實施VPN隧道。但是,大多數小型企業使用經濟高效的寬頻Internet服務(如DSL或電纜

),並從其ISP接收動態IP地址。在這種情況下,可以使用動態域名服務(DDNS)將動態IP地址 對映到完全限定域名(FQDN)。

LAN IP定址 — 每個站點的專用LAN IP網路地址不應重疊。應始終更改每個遠端站點的預設 LAN IP網路地址。

#### 配置提示

#### 預配置核對表

步驟1.在RV320與其DSL或電纜數據機之間連線乙太網電纜,並在ISA570與其DSL或電纜數據 機之間連線乙太網電纜。

步驟2.開啟RV320,然後將內部PC、伺服器及其他IP裝置連線到RV320的LAN埠。 步驟3.開啟ISA570,然後將內部PC、伺服器及其他IP裝置連線到ISA570的LAN埠。 步驟4.確保配置不同子網中每個站點的網路IP地址。在本示例中,遠端辦公室LAN使用 192.168.1.0,而總部LAN使用10.10.10.0。 步驟5.確保本地PC能連線到各自的路由器,並能連線到同一LAN中的其他PC。

#### 識別WAN連線

您需要知道您的ISP是提供動態IP地址還是靜態IP地址。ISP通常提供動態IP地址,但您應在完 成站點到站點VPN隧道配置之前確認這一點。

# 在遠端辦公室為RV320配置站點到站點IPsec VPN隧道

步驟1.轉到VPN > Gateway-to-Gateway(請參閱圖片)

a.) 輸入隧道名稱,例如RemoteOffice。

b.) 將Interface設定為WAN1。

c.) 使用預共用金鑰將Keying Mode設定為IKE。

d.) 輸入本地IP地址和遠端IP地址。

下圖顯示RV320 Gigabit Dual WAN VPN路由器網關到網關頁面:

cisco RV320 Gi	gabit Dual WAN VPN R	outer
Getting Started System Summary	Gateway to Gateway	
▶ Setup	Add a New Tunnel	
► DHCP	Tunnel No.	2
<ul> <li>System Management</li> <li>Port Management</li> </ul>	Tunnel Name:	
▶ Firewall	Interface:	WAN1
VPN Summary	Keying Mode:	IKE with Preshared key
Client to Gateway VPN Passthrough	Local Group Setup	
Certificate Management	Local Security Cateway Type:	IP Only
► Log	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 Ri	ghts Reserved.	

步驟2.設定IPSec隧道設定(請參閱圖片)

a.) 將 Encryption 設定為3DES。

- b.) 將Authentication設定為SHA1。
- c.) 檢查完全向前保密。

d.) 設定*預共用金鑰*(兩台路由器上必須相同)。

下面顯示了IPSec設定(第1階段和第2階段):

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 +		

**附註:**請記住,站點到站點IPsec VPN隧道兩端的IPsec隧道設定必須匹配。如果RV320和 ISA570的IPsec隧道設定之間存在任何差異,則兩台裝置都將無法協商加密金鑰並且無法連線

步驟3.按一下Save以完成設定。

# 在主辦公室為ISA570配置站點到站點IPsec VPN隧道

步驟1.轉到VPN > IKE Policies (請參閱圖片)

- a.) 將 Encryption 設定為 ESP\_3DES。
- b.) 將Hash設定為SHA1。
- c.) 將Authentication設定為Pre-shared Key。
- d.) 將D-H Group設定為Group 2(1024位)。
- 下圖顯示IKE策略:

Small Business cisco ISA500 Series Col	nfigu	uration Utility					11.1.2 (11.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1	
Configuration Wizards	IKE	Policies						
Status	IKE	Dolicies						
Networking								
Firewall		L'Add 💙 Delete						
Security Services	닏	Name	Encr	yption		Hash	Authentication	D-H Group
VPN		Defaultike	AES_	256		ена1		group_2
<ul> <li>VPN Status</li> </ul>		IV320	3DE	IKE Policy - A	dd/Edit		<b>TEU</b>	group_2
IPsec VPN Status				Name:	rv320			
SSL VPN Status				Encryption:	ESP 3D	ES 🔽		
✓ Site-to-Site				Hach:				
IKE Policies				nasii.	0 5	0 1000		
Transform Sets				Authentication	n: • Pre-s	hared Key 🔘 RSA	_SIG	
IPsec Remote Access				D-H Group:	Group 2	(1024bits) 💌		
<ul> <li>SSL Remote User Access</li> </ul>					0	5		
Teleworker VPN Client				Lifetime:	Hou	Min Sec	(Range: 3 minutes to 24 hours)	
L2TP Server		_						
VPN Passthrough	Sav	ve Cancel						
							OK Cancel	
Linero								
Diseis								
Device Management								

#### 步驟2.轉到VPN > IKE Transform Sets(請參閱圖片) a.) 將*Integrity*設定為ESP\_SHA1\_HMAC。 b.) 將*Encryption*設定為ESP\_DES。

下面顯示了IKE轉換集:

Transform Sets			
Add X Delete			
Name	Integrity	Encryption	
DefaultTrans	ESP_SHA1_HMAC	ESP_AES_256	
∐ rv320	ESP_SHA1_HMAC  Transform Set - Add/Edit  Name: 17/320  ESP Integrity: ESP_MD5_HMAC  Encryption: ESP_3DES	ESP_3DES	
	Add X Delete	Add X Delete Name Integrity DefaultTrans ESP_SHA1_HMAC rv320 ESP_SHA1_HMAC Transform Set - Add/Edit Name: rv320 ESP Integrity: ○ ESP_MD5_HMAC • Encryption: ESP_3DES ▼	Imaistorin Sets

步驟3.轉到VPN > IPsec Policies > Add > Basic Settings (請參閱圖片)

- a.) 輸入 Description,例如RV320。
- b.) 將 IPsec Policy Enable設定為On。
- c.) 將 Remote Type設定為Static IP。
- d.) 輸入 *遠端地址*。
- e.) 將 Authentication Method 設定為Pre-Shared Key。
- f.) 將 WAN Interface設定為WAN1。
- g.) 將 Local Network 設定為DEFAULT\_NETWORK。

#### h.) 將 Remote Network 設定為RV320。

下圖顯示IPsec策略基本設定:

Small Business cisco ISA500 Series Co	nfiguration L	Utility	
Configuration Wizards	IPsec Polici	ies	
Conliguration Wi2ards Status Networking Firewall Security Services VPN VPN Status IPsec VPN Status SSL VPN Status SSL VPN Status Site-to-Site IPsec Policies IKE Policies IKE Policies IPsec Remote Access SSL Remote User Access Teleworker VPN Client L2TP Server VPN Passthrough	IPsec Policie	Psec Policies - Add/Edit   selections   or secription:   r320   encote Type:   static IP •   Remote Address:   10.10.10.2   or certificate:   ererificate:   certificate:   default •   WAN Interface:   WAN Interface:   WAN Interface:   DeFAULT_NETWORK •   or secription:   r320 •	IKE IV320
Users			

步驟4.轉到 VPN > IPsec Policies > Add > Advanced Settings(參見圖片)

- a.) 將 IKE Policy和 IKE Transform Sets分別設定為步驟1和2中建立的策略。
- b.) 將 SA-Lifetime設定為0小時5分鐘0秒。
- c.) 按一下「**OK**」(確定)。
- 以下顯示IPsec策略高級設定:

IsA500 Series Configuration Utility					
Configuration Wizards					
Status	tit	Help			
Networking					
Firewall	iced setun		_		
Security Services Windows Networking (Net BIOS) Broadcast	Windows Networking (Net BIOS) Broadcast: O On  Off				
VPN Access Control	I: Zone	e Access Setting	IKE		
v VPN Status	LAN	Permit      Deny	rv320		
IPsec VPN Status	WAN	Deny			
- Site-to-Site	DMZ	Permit Deny			
IPsec Policies	GUES	ST   Permit  Deny			
IKE Policies	SSLV	VPN   Permit  Deny			
Transform Sets	VOICE	CE			
IPsec Remote Access					
SSL Remote User Access     Apply NAT Policies:     Apply NAT Policies:		◯ On ● Off			
L2TP Server Translated Local Ne	etwork:	– Select an address object – 💌			
VPN Passthrough Translated Remote	Network:	– Select an address object – 💌			
Save Cancel IKE Policy:		IKE Policy Link			
Transform:		Transform Link			
SA-Lifetime:		0 Hour 5 Min 0 Sec (Range: 3 minutes to 24 hours)			
lisers		OK Cancel			

步驟5.連線站點到站點IPsec VPN隧道(請參閱圖片)

# a.) 將 *Enable VPN*設定為On。 b.) 按一下 **Connect**按鈕。 下圖顯示「連線」按鈕:

<b>IPsec Policies</b>					
Enable VPN: <ul> <li>O</li> </ul>	n O Off				
IPsec Policies					
🕂 Add 🗙 Delete	🛞 Refresh				
ers	Local	Remote	IKE	Transform	Configure
.10.10.2	*DEFAULT_NETWORK	rv320	rv320	rv320	/ X & &