具有重疊專用網路的兩台IOS路由器之間的 IPsec配置示例

目錄

簡介

本文檔介紹如何在站點到站點IPsec VPN中配置Cisco IOS路由器,在VPN網關後面使用重疊的專用 網路地址。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據執行軟體版本12.4的Cisco IOS 3640路由器。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

慣例

<mark>請參閱<u>思科技術提示慣例以瞭解更多有關文件慣例的資訊。</u></mark>

設定

本節提供用於設定本文件中所述功能的資訊。

註:使用<u>Command Lookup Tool</u>(僅<u>供</u>已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

網路圖表

此文件使用以下網路設定:



注意:此配置中使用的IP編址方案在Internet上不能合法路由。這些地址是在實驗室環境中使用的 RFC 1918地址。

Private_LAN1和Private_LAN2的IP子網均為192.168.1.0/24。這將模擬IPsec通道兩端的重疊地址空間。

在本示例中,Site_A路由器執行雙向轉換,以便兩個專用LAN可以通過IPsec隧道通訊。此轉譯意味 著Private_LAN1透過IPsec通道「看到」Private_LAN2為10.10.10.0/24,而Private_LAN2透過 IPSec通道「看到」Private_LAN1為10.5.5.0/24。

組態

本檔案會使用以下設定:

- <u>站點 A路由器SDM配置</u>
- <u>Site A路由器CLI配置</u>
- <u>Site B路由器配置</u>

站點_A路由器SDM配置

注意:本檔案假定路由器已配置介面配置等基本設定。有關詳細資訊,請參閱<u>使用SDM的基本路由</u> <u>器配置</u>。

NAT配置

完成以下步驟,以便使用NAT在Site_A路由器上配置SDM:

1. 選擇Configure > NAT > Edit NAT Configuration,然後按一下Designate NAT Interfaces以定 義受信任和不受信任的介面,如下所示。

i	89 100 100	Configure	ß	Monitor	Refre	⊧ sh S	iave S		
Va	🐕 NAT								
	Create NAT Configuration Edit NAT Configuration								
	Designate NAT Interfaces.								
N	AT Ir	nterface Se	tting				×		
	Select the list of interfaces that you want to designate as inside / outside.								
		interface		inside(trus	ted)	outside	e(untruste		
	Ethe	ernet0/0							
	Fas	tEthernet1/(ו						
	Loo	pback0		V					
	1						ŀ		
		0	к	Cance		Help			

2. 按一下「OK」(確定)。

3. 按一下Add以配置從內部到外部方向的NAT轉換,如下所示。

Add Address Translation Rule	
💿 Static 💦 O Dynamic	
Direction: From inside to a	outs de 🔄
Translate from interface	
Inside Interface(s):	Loopback0
IP address:	192.168.1.0
Network Mask(optional):	255.255.255.0 or 24
Translate to interface —	
Outside Interface(s):	Ethernet0/0
Type:	IP address 📃
Interface:	Ethernet0/0
IP address:	10.5.5.0
Redirect Port —	
Original Port	Translated Port:
originari ort.	
ок	Cancel Help

4. 按一下「OK」(確定)。

Network Address Translation Rules							
Inside Interface(s): Loopback0							
Outside Interface(s): Ethernet0/0							
Original address		Translated address	Rule Type	Add			
192.168.1.0-192.1	168.1.255	10.5.5.0-10.5.5.255	Static				

5. 再次按一下Add以配置從外部到內部方向的NAT轉換,如下所示。

Add Address Translation Rule	
Static	
Direction: From outside to i	inside 💌
Translate from interface –	
Outside Interface(s):	Ethernet0/0
IP address:	10.10.10.0
Network Mask(optional):	255.255.255.0 or 24
Translate to interface	
Inside Interface(s):	Loopback0
IP address:	192.168.1.0
Redirect Port —	
OTCP OUDP	
Original Port	Translated Port
onginari on.	
ок	Cancel Help

6. 按一下「OK」(確定)。

-							
 Network Address Trar 	Network Address Translation Rules						
Inside Interface(s):	LoopbackO						
Outoido Interfaco/o):	Ethornot0/0						
Outside Internace(s).	Ememetovo						
Original address		Translated address	Rule Type				
192.168.1.0-192.1	68.1.255	10.5.5.0-10.5.5.255	Static				
192.168.1.0-192.1	68.1.255	10.10.10.0-10.10.10.255	Static				

注意:以下是等效的CLI配置:

等效的CLI配置
<pre>interface Loopback0 ip nat inside interface Ethernet0/0 ip nat inside ip nat inside ip nat inside source static network 192.168.1.0 10.5.5.0 /24 ip nat outside source static network 192.168.1.0 10.10.10.0 /24</pre>

VPN配置

完成以下步驟,以便使用VPN在Site_A路由器上配置SDM:

1. 選擇Configure > VPN > VPN Components >IKE > IKE Policies > Add以定義IKE策略,如下 圖所示。

Configure IKE Policy							
Priority:		Authentication:					
Encryption: DES	_	D-H Group: group1					
Hash: MD5	_	Lifetime: 24 0 0 HH:MM:S					
	ок	Cancel	Help				

2. 按一下「OK」(確定)。

IKE Policies						Edit	Del
_							
	Priority	Encryption	Hash	D-H Group	Authentication	Туре	
	10	DES	MD5	aroup1	PRE SHARE	User De	fined

注意:以下是等效的CLI配置:

等效的CLI配置
crypto isakmp policy 10 encr des hash md5 authentication pre-share group1

3. 選擇Configure > VPN > VPN Components >IKE > Pre-shared Keys > Add以使用對等IP地址 設定預共用金鑰值。

Key:	****					
Re-enter Key:	*****					
Host/Networ	′k					
Type:	IP Address 💌					
IP Address:	172.16.1.2					
Subnet Mask: (Optional)	255.255.255.0	24				
User Authentication (XAuth)						
OK	Cancel	Help				

4. 按一下「OK」(確定)。

Pre-shared Keys				
	Peer IP/Name	Subnet Mask	pre-shared key	
	1721612	255 255 255 0	****	

注意:以下是等效的CLI配置:



5. 選擇Configure > VPN > VPN Components > IPSec > Transform Sets > Add以建立轉換集 myset,如下圖所示。

Add Transform Set							
Name:	myset						
✓ Data integrity with encryption (ESP)							
Integrity Algorithm: ESP_MD5_HMAC							
Encryption Algorithm:			ESP_DES		-		
Show Advan							
	OK		Cancel		Help		

6. 按一下「OK」(確定)。

Transform Set			Add
Name	ESP Encryption	ESP Integrity	AH Integrity
myset	ESP_DES	ESP_MD5_HMAC	ata dia dia dia

注意:以下是等效的CLI配置:

等效的CLI配置			
crypto ipsec transform-set myset esp-des esp-md5-hmac			

7. 選擇Configure > VPN > VPN Components > IPSec > IPSec Rules(ACLs)> Add以建立加密訪

問控制清單(ACL)101。

٩dd	a Rule					
	Name/Nun	nber:		Type:		
	101			Exter	nded Rule	9
	Descriptior	1:				
	Rule Entry					
	permit ip 1	0.5.5.0 0.255.	255.255 192.1	168.1.0	0.255.	Add.,
						Clana
						Edit
						Delet
						Delet
						Move U
	•				F	Move Do
	Interfac	e Associatior	î			
	None				Assn	riate
	none.				7,000	erene
		ок	Cancel		Help	

8. 按一下「OK」(確定)。



注意:以下是等效的CLI配置:

				等效的CI	LI配置		
access-list 1	101 r	permit	ip	10.5.5.0	0.0.0.255	192.168.1.0	0.0.0.255

9. 選擇Configure > VPN > VPN Components > IPSec > IPSec Policies > Add以建立加密對映 mymap,如下圖所示。



10. 按一下「Add」。

a. 按一下General頁籤並保留預設設定。

Add Crypto Map
General Peer Information Transform Sets IPSec Rule
Name of IPSec Policy: mymap
Description:
Sequence Number: 1
Security Association Lifetime: 1 0 0 HH:MM:SS Idle Time: Idle Time: HH:MM:SS Perfect Forward Secrecy group1
OK Cancel Help

b. 按一下Peer Information頁籤以新增對等IP地址172.16.1.2。

Add Crypto Map						
General	(Peer Information)	Transform	Sets	IPSec	Rule	
You can have multiple peers in a crypto map. The additional peers are used as backups. Specify Peers						
IP add	ress or hostname		_			
IP address or hostname Current List Add >> Remove						
		Cancel		lein		

c. 按一下Transform Sets頁籤以選擇所需的轉換集myset。



d. 按一下IPSec Rule頁籤以選擇現有加密ACL 101。

General	eer Information	Transform Sets	IPSec Rule
IPSec F	Rule: 101		
			Select an existing
			Create a new rule
			None (Clear rule a
	ок	Cancel	Help

e. 按一下「OK」(確定)。

注意:以下是等效的CLI配置:

等效的CLI配置 crypto map mymap 10 ipsec-isakmp set peer 172.16.1.2 set transform-set myset match address 101

11. 選擇Configure > VPN > Site-to-Site VPN > Edit Site-to-Site VPN > Add,將加密對映 mymap應用到介面Ethernet0/0。



12. 按一下「OK」(確定)。

注意:以下是等效的CLI配置:



Site_A路由器CLI配置

<#root>
Site_A#
show running-config
*Sep 25 21:15:58.954: %SYS-5-CONFIG_I: Configured from console by console Building configuration

```
Current configuration : 1545 bytes
1
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
I
hostname Site_A
I
boot-start-marker
boot-end-marker
i
I
no aaa new-model
i
resource policy
!
i
ï
ip cef
L
1
crypto isakmp policy 10
hash md5
authentication pre-share
!--- Defines ISAKMP policy.
crypto isakmp key 6 L2L12345 address 172.16.1.2 255.255.255.0
!--- Defines pre-shared secret used for IKE authentication
i
L
crypto ipsec transform-set myset esp-des esp-md5-hmac
!--- Defines IPSec encryption and authentication algorithms.
i
crypto map mymap 10 ipsec-isakmp
 set peer 172.16.1.2
 set transform-set myset
match address 101
!--- Defines crypto map.
i
i
ļ
interface Loopback0
 ip address 192.168.1.1 255.255.255.0
```

```
ip nat inside
ip virtual-reassembly
interface Ethernet0/0
ip address 10.1.1.2 255.255.255.0
ip nat outside
ip virtual-reassembly
half-duplex
crypto map mymap
!--- Apply crypto map on the outside interface.
ļ
i
!--- Output Suppressed
ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 10.1.1.1
1
ip nat inside source static network 192.168.1.0 10.5.5.0 /24
!--- Static translation defined to translate Private_LAN1 !--- from 192.168.1.0/24 to 10.5.5.0/24. !--
ip nat outside source static network 192.168.1.0 10.10.10.0 /24
!--- Static translation defined to translate Private_LAN2 !--- from 192.168.1.0/24 to 10.10.10.0/24.
ļ
access-list 101 permit ip 10.5.5.0 0.0.0.255 192.168.1.0 0.0.0.255
!--- Defines IPSec interesting traffic. !--- Note that the host behind Site_A router communicates !---
i
control-plane
ļ
I
line con 0
line aux 0
line vty 0 4
ļ
ļ
```

Site_B路由器CLI配置

Site_B路由器
<#root>
Site_B#
show running_config
Building configuration
Current configuration : 939 bytes
version 12.2 service timestamps debug uptime service timestamps log uptime no service password-encryption !
hostname Site_B !
! ip subnet-zero !
!
crypto isakmp policy 10 hash md5 authentication pre-share
crypto isakmp key L2L12345 address 10.1.1.2 255.255.255.0
! !
crypto ipsec transform-set myset esp-des esp-md5-hmac
!
crypto map mymap 10 ipsec-isakmp set peer 10.1.1.2 set transform-set myset match address 101
! ! !
interface Ethernet0 ip address 192.168.1.1 255.255.255.0 !
interface Ethernet1 ip address 172.16.1.2 255.255.255.0
crypto map mymap

```
!
!
!--- Output Suppressed
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.1.1
ip http server
!
access-list 101 permit ip 192.168.1.0 0.0.0.255 10.5.5.0 0.0.0.255
!
line con 0
line aux 0
line vty 0 4
!
end
Site_B#
```

驗證

本節提供的資訊可用於確認您的組態是否正常運作。

<u>輸出直譯器工具</u>(僅供<u>已註冊</u>客戶使用)(OIT)支援某些show命令。使用OIT檢視show命令輸出的分析 。

• show crypto isakmp sa — 顯示對等體上的所有當前網際網路金鑰交換(IKE)安全關聯(SA)。

<#root>

Site_A#

show crypto isakmp sa

dst	src	state	conn-id slot	status
172.16.1.2	10.1.1.2	QM_IDLE	1 0	ACTIVE

• show crypto isakmp sa detail — 顯示對等體上所有當前IKE SA的詳細資訊。

<#root>
Site_A#
show cryto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection K - Keepalives, N - NAT-traversal X - IKE Extended Authentication psk - Preshared key, rsig - RSA signature

renc - RSA encryption

C-id Local Remote I-VRF Status Encr Hash Auth DH Lifetime Cap. 1 10.1.1.2 172.16.1.2 ACTIVE des md5 psk 1 23:59:42

Connection-id:Engine-id = 1:1(software)

• show crypto ipsec sa — 顯示當前SA使用的設定。

<#root>

Site_A#

show crypto ipsec sa

interface: Ethernet0/0 Crypto map tag: mymap, local addr 10.1.1.2 protected vrf: (none) local ident (addr/mask/prot/port): (10.5.5.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0) current_peer 172.16.1.2 port 500 PERMIT, flags={origin_is_acl,} #pkts encaps: 2, #pkts encrypt: 2, #pkts digest: 2 #pkts decaps: 2, #pkts decrypt: 2, #pkts verify: 2 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0 #pkts not decompressed: 0, #pkts decompress failed: 0 #send errors 3, #recv errors 0 local crypto endpt.: 10.1.1.2, remote crypto endpt.: 172.16.1.2 path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0 current outbound spi: 0x1A9CDC0A(446487562) inbound esp sas: spi: 0x99C7BA58(2580003416) transform: esp-des esp-md5-hmac , in use settings ={Tunnel, } conn id: 2002, flow_id: SW:2, crypto map: mymap sa timing: remaining key lifetime (k/sec): (4478520/3336) IV size: 8 bytes replay detection support: Y Status: ACTIVE inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0x1A9CDC0A(446487562) transform: esp-des esp-md5-hmac , in use settings ={Tunnel, } conn id: 2001, flow_id: SW:1, crypto map: mymap sa timing: remaining key lifetime (k/sec): (4478520/3335) IV size: 8 bytes replay detection support: Y

```
Status: ACTIVE
outbound ah sas:
outbound pcp sas:
Site_A#
```

• show ip nat translations — 顯示轉換插槽資訊。

<#root>

Site_A#

show ip nat translations

Pro	Inside global	Inside local	Outside local	Outside global
			10.10.10.1	192.168.1.1
			10.10.10.0	192.168.1.0
	10.5.5.1	192.168.1.1		
	10.5.5.0	192.168.1.0		

• show ip nat statistics — 顯示有關轉換的靜態資訊。

<#root>

Site_A#

show ip nat statistics

Total active translations: 4 (2 static, 2 dynamic; 0 extended) Outside interfaces: EthernetO/O Inside interfaces: LoopbackO Hits: 42 Misses: 2 CEF Translated packets: 13, CEF Punted packets: 0 Expired translations: 7 Dynamic mappings: Queued Packets: 0 Site_A#

- 完成以下步驟以驗證連線:
 - 1. 在SDM中,選擇Tools > Ping以建立來源IP為192.168.1.1、目的地IP為10.10.10的IPsec VPN通道。

Ping		
* Source:	192.168.1.1	Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 secor
Destination:	10.10.10.1	!! Success rate is 40 percent (2/5), round-trip min/avg/max = 36/38/4
(*) Optional F	ïeld	Clear Output Close Help

2. 按一下Test Tunnel以檢查是否已建立IPsec VPN通道,如下圖所示。

Create	e Site to Site VPN	Edit Site to Site VPN			
					Add
	Status	Interface	Descriptio	n	IPSec Policy
	오 Down	Ethernet0/0			mymap 1
•					•
		C	ear Connection	n (Test Tunnel).	Generate Mirror

3. 按一下「Start」。

VPN Troubleshooting			
Tunnel Details			
Interface: Ethernet0/0	Peer: 172.	16.1.2	
			_
		📃 Summary	🗟 Details
Activity			Status
Checking the tunnel status			🖕 Up
Information		×	
(i) VF	PN Troubleshooting is successful	1	
Th	ne VPN Tunnel is up.		
Failure Rea		(s)	
	OK		
Start	Save Report Close		Help

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

<#root>

Site_A#

```
debug ip packet
```

```
IP packet debugging is on
Site_A#ping
Protocol [ip]:
Target IP address: 10.10.10.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [OxABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
```

Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds: Packet sent with a source address of 192.168.1.1 !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 40/45/52 ms Site_A# *Sep 30 18:08:10.601: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethern et0/0), routed via FIB *Sep 30 18:08:10.601: IP: s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), len 100, sending *Sep 30 18:08:10.641: IP: tableid=0, s=10.10.10.1 (Ethernet0/0), d=192.168.1.1 (Loopback0), routed via RIB *Sep 30 18:08:10.641: IP: s=10.10.10.1 (Ethernet0/0), d=192.168.1.1, len 100, rc vd 4 *Sep 30 18:08:10.645: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethern et0/0), routed via FIB *Sep 30 18:08:10.645: IP: s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), len 100, sending *Sep 30 18:08:10.685: IP: tableid=0, s=10.10.10.1 (Ethernet0/0), d=192.168.1.1 (Loopback0), routed via RIB *Sep 30 18:08:10.685: IP: s=10.10.10.1 (Ethernet0/0), d=192.168.1.1, len 100, rc vd 4 *Sep 30 18:08:10.685: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethern et0/0), routed via FIB *Sep 30 18:08:10.689: IP: s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), len 100, sending *Sep 30 18:08:10.729: IP: tableid=0, s=10.10.10.1 (Ethernet0/0), d=192.168.1.1 (Loopback0), routed via RIB *Sep 30 18:08:10.729: IP: s=10.10.10.1 (Ethernet0/0), d=192.168.1.1, len 100, rc vd 4 *Sep 30 18:08:10.729: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethern et0/0), routed via FIB *Sep 30 18:08:10.729: IP: s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), len 100, sending *Sep 30 18:08:10.769: IP: tableid=0, s=10.10.10.1 (Ethernet0/0), d=192.168.1.1 (Loopback0), routed via RIB *Sep 30 18:08:10.769: IP: s=10.10.10.1 (Ethernet0/0), d=192.168.1.1, len 100, rc vd 4 *Sep 30 18:08:10.773: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethern et0/0), routed via FIB *Sep 30 18:08:10.773: IP: s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), len 100, sending *Sep 30 18:08:10.813: IP: tableid=0, s=10.10.10.1 (Ethernet0/0), d=192.168.1.1 (Loopback0), routed via RIB *Sep 30 18:08:10.813: IP: s=10.10.10.1 (Ethernet0/0), d=192.168.1.1, len 100, rc vd 4

相關資訊

- <u>最常見的L2L和遠端訪問IPSec VPN故障排除解決方案</u>
- 具有重疊專用網路的ASA/PIX和Cisco VPN 3000集中器之間的IPSec配置示例
- 技術支援與文件 Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。