

10-6-2 ISAKMP 安全套件



✦ ISAKMP Phase 1 :

	參數	L_R1	R_R2
鑰匙分配方法	Manual or ISAKMP	ISAKMP	ISAKMP
加密演算法	DES、3DES、 ASE	AES	AES
雜湊演算法	MD5、 SHA-1	SHA-1	SHA-1
認證方法	Pre-shared 、RSA	Pre-share	Pre-share
鑰匙交換	DH Group1、 2 、5	DH 2	DH 2
IKE Lifetime	86400 Sec. or less	86400	86400
ISAKMP Key	(自行定義)	csuMIS	csuMIS

✦ ISAKMP Phase 2 :

	參數	L_R1	R_R2
安全套件名稱 (自行定義)	VPN-SET	VPN-SET	VPN-SET
安全套件內容：IPSec 協定	ESP-AES、ESP-SHA-HMAC	ESP-AES、ESP-SHA-HMAC	ESP-AES、ESP-SHA-HMAC
對方主機	R_R2	L_R1	L_R1
對方 IP 位址	10.100.1.1	10.100.2.1	10.100.2.1
加密網路範圍	140.100.1.0/24	140.100.2.0/24	140.100.2.0/24
網路範圍名稱 (自行定義)	VPN-MAP	VPN-MAP	VPN-MAP
SA 建立方法	ipsec-isakmp	ipsec-isakmp	ipsec-isakmp

