1 Introduction

This application note details the steps for creating VPN tunnels based on "hub and spoke" topology between ASUS Internet Security Routers. All settings and screen dumps contained in this application note are taken from ASUS Internet Security Routers running firmware 1.1.68A.410. However, the instructions are applicable to newer firmware as well.

In the "hub and spoke" VPN topology, all branch offices connect to the central office and each office is able to connect to resources on the central network, as well as other offices, by going through their local VPN gateway to link to the central office.



It is recommended that you disable firewall initially to simplify the configuration procedure when setting up "hub-and-spoke" VPN. You can then create proper ACL rules based on secure requirement in your network.

2 Dynamic IP for All Branch Offices

This topology allows all branch offices to use dynamic IP to construct a fully meshed VPN networks. Note that only the headquarter requires static IP.

2.1 Network Setup

Connect all the devices as indicated in Figure 2.1. You may change the IP address, subnet mask and default gateway IP address of any device to match your true network environment.



Figure 2.1. Network Toppology Diagram – Dynamic IP for All Branch Offices

2.2 Setup IPSec VPN for Branch A

The set up procedure involves:

Create a VPN policy, A_HUB, for the tunnel between Branch A and the Headquarter

Configure VPN Rule for the Tunnel between Branch A and the Headquarter

Configuration Parameters	Value	Comment
Site-to-Site	Selected	
Enable	Selected	
Tunnel Name	A_HUB	
Local Secure Group	Subnet 192.168.21.0 255.255.255.0	LAN of Branch A
Remote Secure Group	Any	
Remote Gateway	IP Address 66.228.128.1	WAN IP of Headquarter Gateway
Local ID	E-Mail user_a@asus.com.tw	
Remote ID	None	
Preshared Key	1234	

ID T:A_HUB ♥ Name AHUB ● Enable ○ Disable Move to 1 ♥ VPN Connection Type ● Site to Site ○ Remote Access VPN Keep Alive ○ Enable ● Disable Local Secure Group Subnet ♥ Local Secure Group Type Any ♥ Local Gateway Interface etho ♥ Remote Gateway Interface etho ♥ Fype PAddress ● IP Address ● 6 228128.1 Local ID Type E-Mail ♥ E-Mail User_a@asus con.tw Remote ID Type None ♥ Key Management Preshared Key ♥ KE Mode ○ Main ● Aggressive Xauth ○ Enable ● Disable Preshared Key ♥ KE Encryption/Authentication ALL ♥ Life Time 3000 sec ♥ IPSec Proposal Settings IPSec Encryption/Authentication ALL ♥ Iffe Time 3600 Sec ♥ or 75000 KByte Iffe Time 3600 Sec ♥ or 75000 KByte Iffe Time 5600 Sec ♥ or 75000			VPN C	onnection Set	ttings			
VPN Connection Type Iso Site to Site Remote Access VPN Keep Alive O Enable Disable Type Subnet Iso Subnet Subnet Iso Address Subnet Iso Subnet Iso Iso Local Secure Group Type Any Local Gateway Interface eth0 Iccal ID Type IP Address E-Mail User_a@asus.com.tw Remote ID Type None Key Management Preshared Key Itke Proposal Settings IKE Proposal Settings IKE Proposal Settings IKE Encryption/Authentication ALL ✓ Left Filme 3600 see IPSec Encryption/Authentication ALL ✓ Chained Authentication Header O None ✓ Operation Mode O Tunnel O Transport PFS Group None ✓ Iffe Time 3600 See or Iffe Time 3600 See or Iffe Time 3600 See	ID 1: A_HUB 💌	Nam	ne A_HUB		 Enable 	O Disable	Move t	to 1 🕶
VPN Keep Alive O Enable O Isable Type Subnet Subnet Address Subnet 192188.21.0 Subnet Mask 255.255.255.0 Remote Secure Group Type Anv Local Gateway Interface eth0 Remote Gateway Type IP Address ID Type E-Mail Image: Secure Group Type Interface eth0 Image: Secure Group Remote Gateway Type IP Address Image: Secure Group Local ID Type E-Mail Image: Secure Group Key Management Preshared Key Image: Secure Group Image: Secure Group KE Mode O Main O Aggressive Xauth O Enabled Preshared Key Image: Sec Proposal Settings Image: Secure Group Image: Secure Group KE Encryption/Authentication ALL Image: Secure Group Image: Secure Group Image: Secure Group PSec Encryption/Authentication ALL Image: Secure Group	VPN Connection	Туре	⊙ Site to Site	O Remote Ac	cess			
Local Secure Group Type Subnett Subnett 192.188.21.0 Subnett Address Subnett Subnett Mask 255.255.255.0 Remote Secure Group Type Interface eth0 v Local Gateway Interface IP Address # PAddress # PAddress # Remote Gateway Type IP Address # E-Mail w Local ID Type E-Mail user_a@asus.com.tw Remote ID Type None V Key Management Preshard Key V IKE Proposal Settings V Key Management Oreabled Preshared Key exe Vauth © Enabled Preshared Key exe VE Encryption/Authentication ALL Ufe Time 3800 sec v PSec Encryption/Authentication ALL Chained Authentication Header O None AH MD-5 Operation Mode O Tunnel O Transport	VPN Keep Alive		OEnable	💿 Disable				
Local Secure Group Subnet Address 192.168.21.0 Subnet Mask 265.255.25.0 Remote Secure Group Type Local Gateway Interface eth0 ✓ Remote Gateway Type IP Address ● Local ID Type E-Mail ✓ E-Mail ✓ Local ID Type Remote ID Type Type None Key Management Preshared Key V ● KE Mode O Main O Enabled ● Disabled Preshared Key ● IKE Encryption/Authentication ALL V ● PSec Encryption/Authentication ALL Chained Authentication Header O None O Prestored ● Ver I ● If F Time 3600 Sec ♥ or 75000 KByte If F Time 3600 Sec ♥ or 75000 KByte If Time 3600 Sec ♥ or 75000 Key Mgmt.			Туре	Subnet 🗸 🗸				
Subnet Mask 255.255.0 Remote Secure Group Type Any Interface eth0 Interface Type P Address Paddress IP Address IP Address 66.2281.28.1 Local ID Type E-Mail User_a@asus.com.tw Remote ID Type Key Management Preshared Key Vex Oman Angressive Xauth Vershared Key Imagement Preshared Key Imagement If e Time 3600 sec Imagement PSec Encryption/Authentication ALL Imagement Chained Authentication Header O None O AH SHA-1 O AH MD-5 Operation Mode Tunnel O Transport Thep PFS Group None Imagement Modify Delete Help <td>Local Secure Gro</td> <td>oup</td> <td>Subnet Address</td> <td>192.168.21.0</td> <td></td> <td></td> <td></td> <td></td>	Local Secure Gro	oup	Subnet Address	192.168.21.0				
Remote Secure Group Type Any ✓ Local Gateway Interface @th0 ✓ Remote Gateway IP Address Ø6.228.128.1 ✓ Local ID Type E-Mail ✓ Remote ID Type None ✓ Remote ID Type None ✓ Key Management Preshared Key ✓ ✓ IKE Mode O Main O Aggressive ✓ Xauth O Enabled O Isabled ✓ Preshared Key ● ● ✓ IKE Encryption/Authentication ALL ✓ ✓ Ife Time 3600 sec ♥ ✓ PSec Encryption/Authentication ALL ✓ ✓ Chained Authentication Header O None O AH SHA-1 O AH MD-5 Operation Mode O Tunnel O Transport ✓ PFS Group None ✓ Keyte Help Idf Modify Delete Help Site to Site Access Eules Idd Mode XAUTH Status ID N			Subnet Mask	255.255.255.0				
Local Gateway Interface eth0 ▼ Remote Gateway Type IP Address ● IP Address 66.228.128.1 ● Local ID Type E-Mail ▼ Remote ID Type None ▼ Key Management Preshared Key ▼ Vey Management Preshared Key ▼ IKE Proposal Settings IKE Proposal Settings IKE Mode O Main O Aggressive Xauth O Enabled O Isabled Preshared Key ● ● IKE Encryption/Authentication ALL ▼ Life Time 3600 sec ♥ IPSec Encryption/Authentication ALL ▼ Chained Authentication Header O None ○ AH SHA-1 O AH MD-5 Operation Mode O Tunnel ○ Transport ● PFS Group None ♥ Life Time 3600 Sec ♥ or 75000 KByte ILfe Time 3600 Sec ♥ or 75000 KByte ILfe Time 3600 Sec ♥ or 75000 KByte ILfe Time <td>Remote Secure C</td> <td>Group</td> <td>Туре</td> <td>Any 🗸</td> <td></td> <td></td> <td></td> <td></td>	Remote Secure C	Group	Туре	Any 🗸				
Remote Gateway Type IP Address IP Address IP Address 66.228.128.1 Local ID Type E-Mail Image: Stress and	Local Gateway		Interface	eth0 💌				
Remote Object IP Address 66.228.128.1 Local ID Type E-Mail ✓ Remote ID Type None ✓ Key Management Preshared Key ✓ ✓ IKE Mode Main ◇ Aggressive ✓ Xauth ○ Enabled ○ Disabled ✓ Preshared Key ● ● ✓ IKE Encryption/Authentication ALL ✓ ✓ Iffer Time 3800 sec ♥ ✓ IPSec Encryption/Authentication ALL ✓ ✓ Chained Authentication Header ○ None ○ AH SHA-1 ○ AH MD-5 Operation Mode ○ Tunnel ○ Transport ✓ PFS Group None ✓ ✓ ✓ Id Made Group Name Local Network Mode XAUTH Status Site to Site Access List Rules IPSec Status ID Name Local/Remote Network Tunnel End- point Key Mgmt. IPSec Status ID Name Local/Remote Network Gotta	Demote Cateway		Туре	IP Address 🐱				
Local ID Type E-Mail user_a@asus.com.tw Remote ID Type None ✓ Key Management Preshared Key ✓ IKE Proposal Settings IKE Mode O Main O Aggressive Xauth O Enabled O Disabled Preshared Key ● ● Xauth O Enabled O Disabled Preshared Key ● ● KE Encryption/Authentication ALL ● Life Time 3600 sec ● IPSec Encryption/Authentication ALL ● Chained Authentication Header O None ○ AH SHA-1 ○ AH MD-5 Operation Mode O Tunnel ○ Transport ● PFS Group None △ ✓ ● Life Time 3600 Sec ♥ or 75000 KByte ● Id Name Group Name Local Network Mode XAUTH Status ID Name Local/Remote Network Tunnel End- point Key Mgmt. IPSec Status ID Name <t< td=""><td>Remote Galeway</td><td></td><td>IP Address</td><td>66.228.128.1</td><td></td><td></td><td></td><td></td></t<>	Remote Galeway		IP Address	66.228.128.1				
E-Mail user_a@asus.com.tw Remote ID Type None ✓ Key Management Preshared Key ✓ IKE Proposal Settings ✓ IKE Mode ✓ Main ✓ Aggressive Xauth ✓ Enabled ✓ Disabled Preshared Key ●●●●● ●●●●● IKE Encryption/Authentication ALL ✓ Life Time 3800 sec ✓ IPSec Proposal Settings IPSec Encryption/Authentication ALL ✓ Chained Authentication Header None ◇ AH MD-5 Operation Mode ● Tunnel ○ Transport PFS Group None ✓ Life Time 3600 Sec ✓ or 75000 KByte ✓ ID Name Group Name Local Network Modify Delete Help ID Name Local/Remote Network Tunnel End- point Key Mgmt IPSec Status ID Name Local/Remote Network Tunnel End- point ID Name Local/Remote Network<	LocaLID		Туре	E-Mail 🗸 🗸				
Remote ID Type None ✓ Key Management Preshared Key ✓ IKE Proposal Settings IKE Mode Main Aggressive Xauth O Enabled Disabled Preshared Key ●●●● IKE Encryption/Authentication ALL ✓ Life Time 3600 see ✓ IPSec Proposal Settings IPSec Encryption/Authentication ALL ✓ Chained Authentication Header Ø None O AH SHA-1 O AH MD-5 Operation Mode ● Tunnel O Transport PFS Group None ✓ Life Time 3600 See ✓ or 75000 KByte Remote Access Rules ID Name Group Name Local Network Mode XAUTH Status ID Name Local/Remote Network Tunnel End- point Key Mgmt. IPSec Status ID 192.168.21.0/24 66.228.128.1 Preshared Tunnel Enable	Locario		E-Mail	user_a@asus.c	com.tw			
Key Management Preshared Key ♥ IKE Proposal Settings IKE Mode O Main ● Aggressive Xauth O Enabled ● Disabled Preshared Key ●●●● IKE Encryption/Authentication ALL ♥ Life Time 3600 sec ♥ IPSec Proposal Settings IPSec Encryption/Authentication ALL ♥ Chained Authentication Header None ○ AH SHA-1 ○ AH MD-5 Operation Mode ● Tunnel ○ Transport PFS Group None ♥ Life Time 3600 Sec ♥ or 75000 KByte Remote Access Rules ID Name Group Name Local Network Mode XAUTH ID Name Local/Remote Network Tunnel End- point ID 192.168.21.0/24 An	Remote ID		Туре	None 🗸				
IKE Proposal Settings IKE Mode	Key Management	t	Preshared Key 🗸	•				
IKE Mode O Main ● Aggressive Xauth ○ Enabled ● Disabled Preshared Key •••• IKE Encryption/Authentication ALL Life Time 3600 sec ♥ IPSec Proposal Settings IPSec Encryption/Authentication ALL ♥ Chained Authentication ALL ♥ Chained Authentication Header O None ○ AH SHA-1 ○ AH MD-5 Operation Mode ● Tunnel Transport PFS Group None ○ Life Time 3600 Sec ♥ or 75000 KByte Remote Access Rules ID Name Group Name Local Network Mode XAUTH Status ID Name Local/Remote Network Tunnel End- point Key Mgmt. IPSec Status ID Name Local/Remote Network Tunnel End- point Key Mgmt. IPSec Status I 1 A_HUB 192.168.21.0/24 Any 66.228.128.1 Preshared Tunnel Enable			IKE F	Proposal Setti	ngs			
Xauth ○ Enabled ○ Disabled Preshared Key ••••• I IKE Encryption/Authentication ALL ✓ Life Time 3600 sec ♥ IPSec Proposal Settings IPSec Encryption/Authentication ALL ✓ Chained Authentication Header None ○ AH SHA-1 ○ AH MD-5 Operation Mode ○ Tunnel ○ Transport PFS Group Life Time 3600 Sec ♥ or 75000 KByte Emote Access Rules ID Name Group Name Local Network Mode XAUTH Status ID Name Local/Remote Network Tunnel End- point Key Mgmt. IPSec Status ID Name Local/Remote Network Tunnel End- point Key Mgmt. IPSec Status ID Name Local/Remote Network Tunnel End- point Key Mgmt. IPSec Status ID 1 A_HUB 192.168.21.0/24 Any 66.228.128.1 Preshared Tunnel Enable	IKE Mode		🔘 Main 🛛 💿	Aggressive				
Preshared Key ■●●● IKE Encryption/Authentication ALL ● Life Time 3600 sec ♥ ■ IPSec Proposal Settings IPSec Encryption/Authentication ALL ● Chained Authentication Header ● None ○ AH SHA-1 ○ AH MD-5 ● Operation Mode ● Tunnel ○ Transport ● PFS Group None ♥ ■ Life Time 3600 Sec ♥ or 75000 KByte ● Add Modify Delete ● Øroup None ♥ ■ ● ● Life Time 3600 Sec ♥ or 75000 KByte ● ● Øroup Name Local Network Mode XAUTH Status Site to Site Access Rules ● ● ● ID Name Local/Remote Network Tunnel End-point Key Mgmt. IPSec Status ID Name Local/Remote Network Tunnel End-point Key Mgmt. IPSec Status ID Name Local/Remote Network Tunnel End-point Key Mgmt. IPSec Status ID 1 A_HUB 192.168.21.0/24 Any 66	Xauth		O Enabled	Disabled				
IKE Encryption/Authentication ALL ▼ Life Time 3600 sec ♥ IPSec Proposal Settings IPSec Encryption/Authentication ALL ▼ Chained Authentication Header None OAH SHA-1 OAH MD-5 ✓ Operation Mode ● Tunnel O Transport ✓ PFS Group None ♥ ✓ Life Time 3600 Sec ♥ or 75000 KByte ✓ Add Modify Delete Help Remote Access Rules Terminel Group Name Local Network Mode XAUTH Status Site to Site Access List Rules ID Name Local/Remote Network Tunnel End-point ID Name Local/Remote Network Tunnel End-point ID Name Local/Remote Network Tunnel End-point ID Name Local/Remote Network Tunnel End-point ID Name Local/Remote Network Tunnel End-point ID Name Local/Remote Network Preshared Tunnel End-point ID Name Local/Remote Network Preshared Tunnel End-point Key Mgmt. IPSe	Preshared Key		••••					
Life Time 3600 sec ♥ IPSec Proposal Settings IPSec Encryption/Authentication ALL ♥ Chained Authentication Header None OAH SHA-1 OAH MD-5 Operation Mode Operation Mode Tunnel O Transport PFS Group PFS Group None ♥	IKE Encryption/Au	uthentication	ALL	*				
IPSec Proposal Settings IPSec Encryption/Authentication ALL ✓ Chained Authentication Header None ○ AH SHA-1 ○ AH MD-5 Operation Mode Operation Mode ● Tunnel ○ Transport PFS Group Deration Mode ● Tunnel ○ Transport PFS Group Life Time 3600 Sec ♥ or 75000 KByte Add Modify Delete Help Remote Access Rules ID Name Group Name Local Network Mode XAUTH Status ID Name Local/Remote Network Tunnel End- point Key Mgmt. IPSec Status ID 1 A_HUB 192.168.21.0/24 Any 66.228.128.1 Preshared Tunnel Enable	Life Time		3600 sec 💊	*				
IPSec Encryption/Authentication ALL ▼ Chained Authentication Header None AH SHA-1 AH MD-5 Operation Mode Tunnel Transport PFS Group None Tunnel Transport PFS Group None Tunnel Transport PFS Group None Transport Life Time 3600 Sec or 75000 KByte Add Modify Delete Help Remote Access Rules ID Name ID Name Cocal/Remote Network Tunnel End- point Key Mgmt. IPSec Status 1 A_HUB 192.168.21.0/24 Any 66.228.128.1 Preshared Tunnel Enable			IPSec	Proposal Set	tings			
Chained Authentication Header ● None ● AH SHA-1 ● AH MD-5 Operation Mode ● Tunnel ● Transport PFS Group None ● Life Time 3600 Sec or 75000 KByte Add Modify Delete Help Add Modify Delete ID Name Group Name Local Network Mode XAUTH Site to Site Access Rules ID Name Local/Remote Network Tunnel End- point Key Mgmt. IPSec Status ID 1 A_HUB 192.168.21.0/24 Any 66.228.128.1 Preshared Tunnel Enable	IPSec Encryption.	/Authentication	ALL			*		
Operation Mode Tunnel Transport PFS Group None ✓ Life Time 3600 Sec ✓ or 75000 KByte Add Modify Delete Help Add Modify Delete Help Remote Access Rules ID Name Group Name Local Network Mode XAUTH Status Site to Site Access List Rules ID Name Local/Remote Network Tunnel End- point Key Mgmt. IPSec Status ID 1 A_HUB 192.168.21.0/24 Any 66.228.128.1 Preshared Tunnel Enable	Chained Authenti	ication Header	⊙None ○A	H SHA-1 🛛 🔘	AH MD-5			
None None Life Time 3600 Sec ♥ or 75000 KByte Add Modify Delete Help Add Modify Delete Help Remote Access Rules ID Name Group Name Local Network Mode XAUTH Status Site to Site Access List Rules ID Name Local/Remote Network Tunnel End- point Key Mgmt. IPSec Status Image: 1 A_HUB 192.168.21.0/24 Any 66.228.128.1 Preshared Tunnel Enable	Operation Mode		💿 Tunnel 🛛 🔘	Transport				
Life Time 3600 Sec v or 75000 KByte Add Modify Delete Help Remote Access Rules ID Name Group Name Local Network Mode XAUTH Status Site to Site Access List Rules ID Name Local/Remote Network Tunnel End- point Key Mgmt. IPSec Status ✓ 1 A_HUB 192.168.21.0/24 66.228.128.1 Preshared Tunnel Enable	PFS Group		None 🐱					
Add Modify Delete Help Remote Access Rules ID Name Group Name Local Network Mode XAUTH Status Site to Site Access List Rules ID Name Local/Remote Network Tunnel End-point Key Mgmt. IPSec Status ID Name 192.168.21.0/24 Any 66.228.128.1 Preshared Tunnel Enable	Life Time		3600 Sec 💊	or 75000	KByte			
Remote Access Rules ID Name Group Name Local Network Mode XAUTH Status Site to Site Access List Rules ID Name Local/Remote Network Tunnel End-point Key Mgmt. IPSec Status ID Name 192.168.21.0/24 Any 66.228.128.1 Preshared Tunnel Enable			Ad	d Modify	Delete			Help
ID Name Group Name Local Network Mode XAUTH Status ID Name Local/Remote Network Tunnel End- point Key Mgmt. IPSec Status Image:			Rem	ote Access P	ules			
Site to Site Access List Rules ID Name Local/Remote Network Tunnel End- point Key Mgmt. IPSec Status Image: Marcine State Stat	ID	Name	Group Name	Local Net	work	Mode	XAUTH	Status
ID Name Local/Remote Network Tunnel End- point Key Mgmt. IPSec Status 1 A_HUB 192.168.21.0/24 Any 66.228.128.1 IPSec Status			Site to S	ite Access Lis	st Rules			
	ID	Name	Local/Remote Ne	etwork	Tunnel End point	l- Key N	/Igmt. IP	Sec Status
•	🧨 📅 1	A_HUB	192.168.21.0/24 Any		66.228.128.	1 Presh	ared T	unnel Enable

2.3 Setup IPSec VPN for Branch B

The set up procedure involves:

Create a VPN policy, B_HUB, for the tunnel between Branch B and the Headquarter

Configure VPN Rule for the Tunnel between Branch B and the Headquarter

Configuration Parameters	Value	Comment
Site-to-Site	Selected	
Enable	Selected	
Tunnel Name	B_HUB	

Copyright 2003, ASUSTek Computer, Inc.

Local Secure Group	Subnet 192.168.22.0 255.255.255.0	LAN of Branch B
Remote Secure Group	Any	
Remote Gateway	IP Address 66.228.128.1	WAN IP of Headquarter Gateway
Local ID	E-Mail user_b@asus.com.tw	
Remote ID	None	
Preshared Key	abcd	

VPN Connection Settings					
ID 1: B_HUB 🖌 Nam	B_HUB		⊙Enable C	Disable	Move to 1 🐱
VPN Connection Type	Oite to Site	O Remote A	ccess		
VPN Keep Alive	OEnable	📀 Disable			
Local Secure Group	Type Subnet Address Subnet Mask	Subnet 192.168.22.0 255.255.255.0			
Remote Secure Group	Туре	Any 💊			
Local Gateway	Interface	eth0 💌			
Remote Gateway	Type IP Address	IP Address 💊 66.228.128.1			
Local ID	Type E-Mail	E-Mail 💊 user_b@asus]	
Remote ID	Туре	None 💊			
Key Management	Preshared Key	,			
	IKE	Proposal Set	tings		
IKE Mode	O Main 🧕 🧕	Aggressive			
Xauth	O Enabled (Disabled			
Preshared Key	••••				
IKE Encryption/Authentication	ALL	~			
Life Time	3600 sec	*			
	IPSec	Proposal Se	ttings		
IPSec Encryption/Authentication	ALL			*	
Chained Authentication Header	⊙None ⊙A	AH SHA-1 (AH MD-5		
Operation Mode	⊙ Tunnel C) Transport			
PFS Group	None 🗸				
Life Time	3600 Sec •	or 75000	KByte		
	A	ld Modify	Delete		Help
	Rem	ote Access R	lules		
ID Name	Group Name	Local Ne	twork	Mode	XAUTH Status
	Site to S	iite Access L	ist Rules		
ID Name	Local/Remote N	etwork	Tunnel End- point	Key M	gmt. IPSec Status
🖋 🛅 1 B_HUB	192.168.22.0/24 Any		66.228.128.1	Presha	red Tunnel Enable

2.4 Setup IPSec VPN for Branch C

The set up procedure involves:

Create a VPN policy, C_HUB, for the tunnel between Branch C and the Headquarter

Configure VPN Rule for the Tunnel between Branch C and the Headquarter

Configuration Parameters	Value	Comment
Site-to-Site	Selected	
Enable	Selected	
Tunnel Name	C_HUB	
Local Secure Group	Subnet 192.168.23.0 255.255.255.0	LAN of Branch C
Remote Secure Group	Any	
Remote Gateway	IP Address 66.228.128.1	WAN IP of Headquarter Gateway
Local ID	E- Mail user_c@asus.com.tw	
Remote ID	None	
Preshared Key	5678	

	VPN Connection Settings					
ID 1: C_HUB 🔽 Name	C_HUB		Enable	O Disable	Move to	o 1 🗸
VPN Connection Type	Site to Site Site	O Remote Acc	ess			
VPN Keep Alive	O Enable	 Disable 				
	Туре	Subnet 🗸 🗸				
Local Secure Group	Subnet Address	192.168.23.0				
	Subnet Mask	255.255.255.0				
Remote Secure Group	Туре	Any 🗸				
Local Gateway	Interface	eth0 🔽				
Demote Octowny	Туре	IP Address 🐱				
Remote Galeway	IP Address	66.228.128.1				
LessLID	Туре	E-Mail 🗸 🗸				
Lucario	E-Mail	user_c@asus.c	om.tw			
Remote ID	Туре	None 🔽				
Key Management	Preshared Key 🗸					
	IKE F	Proposal Settii	igs			
IKE Mode	🔘 Main 🛛 💽	Aggressive				
Xauth	O Enabled	Disabled				
Preshared Key	••••					
IKE Encryption/Authentication	ALL	*				
Life Time	3600 sec 🖍	*				
	IPSec	Proposal Sett	ings			
IPSec Encryption/Authentication	ALL			*		
Chained Authentication Header	⊙None ○A	H SHA-1 🛛 🔿	AH MD-5			
Operation Mode	💿 Tunnel 🛛 🔘	Transport				
PFS Group	None 🔽					
Life Time	3600 Sec 💊	or 75000 🛛 🗸	Byte			
	Ac	d Modify	Delete			Help
	Rem	ote Access Ru	les			
ID Name	Group Name	Local Net	work	Mode	XAUTH	Status
	Site to S	ite Access Lis	Rules			
ID Name L	.ocal/Remote N	etwork	Funnel End point	- Key N	lgmt. IPs	Sec Status
🖋 🛅 1 C_HUB 🕺	92.168.23.0/24 my		66.228.128.	1 Presh	ared Tu	nnel Enable

2.5 Setup IPSec VPN for the Headquarter

The set up procedure involves:

Create a VPN policy, HUB_A, for the tunnel between the Headquarter and Branch A Create a VPN policy, HUB_B, for the tunnel between the Headquarter and Branch B Create a VPN policy, HUB_C, for the tunnel between the Headquarter and Branch C

Configure VPN Rule for the Tunnel between the Headquarter and Branch A

Configuration Parameters	Value	Comment
Site-to-Site	Selected	
Enable	Selected	

Tunnel Name	HUB_A	
Local Secure Group	Any	
Remote Secure Group	Subnet 192.168.21.0 255.255.255.0	LAN of Branch A
Remote Gateway	Any	Since WAN IP of Branch A gateway is not known in advance, use "Any" to designate the WAN IP of Branch A gateway
Local ID	None	
Remote ID	E-Mail user_a@asus.com.tw	ID of Branch A
Preshared Key	1234	

				VPN C	onnection	Settings			
ID 1	: HUB	LA 🔽	N	ame HUB_A		💿 Enable 🌔) Disable	Move to 1	*
VPN	Conn	ection	Туре	⊙ Site to Site	○ Remote	Access			
VPN	Кеер	Alive		○ Enable	 Disable 				
Loca	I Sec	ure Gr	oup	Туре	Any	~			
Rem	ote S	ecure	Group	Type Subnet Address Subnet Mask	Subnet 192.168.21 255.255.25	• .0 5.0			
Loca	il Gati	eway		Interface	eth0 🗸				
Rem	ote G	atewa	/	Туре	Any	~			
Loca	II ID			Туре	None	*			
Rem	ote IC)		Type E-Mail	E-Mail user_a@a:	sus.com.tw]		
Key I	Mana	gemer	it	Preshared Key 💊	*				
				IKE I	Proposal S	ettings			
IKE N	Node			O Main 🧕 🧕	Aggressive	е — — — — — — — — — — — — — — — — — — —			
Xauti	h			O Enabled (Disabled				
Pres	hared	t Key		••••					
IKE E	Encry	ption/A	uthentication	ALL	×				
Lite	IIme			3600 Sec	Drenecal	Pottinuo			
IPSe	c Enc	rvotior	N/Authenticatior	n ALL	Proposal	settings	*		
Chai	ned A	Authen	tication Header	· · · · · · · · · · · · · · · · · · ·	AH SHA-1	O AH MD-5			
Oper	ration	Mode		⊙ Tunnel O) Transport				
PFS	Grou	р		None 🗸					
Life 1	Time			3600 Sec 🔹	🖌 or 75000	KByte			
				A	ld Modif	y Delete			Help
				Rem	ote Acces	s Rules			
		ID	Name	Group Name	Local	Network	Mode	XAUTH	Status
				Site to S	ite Access	List Rules			
		ID	Name	Local/Remote N	etwork	Tunnel End- point	Key Mg	jmt. IPSec	: Status
ø	Ē	1	HUB_A	Any 192.168.21.0/24		Any	Preshar	ed Tunne	el Enable
di P	Ē	2	HUB_B	Any 192.168.22.0/24		Any	Preshar	red Tunne	el Enable
e la compañía de la c	Ē	з	HUB_C	Any 192.168.23.0/24		Any	Preshar	red Tunne	el Enable

Configure VPN Rule for the Tunnel between the Headquarter and Branch B

Configuration Parameters	Value	Comment		
Site-to-Site	Selected			
Enable	Selected			
Tunnel Name	HUB_B			
Local Secure Group	Any			
Remote Secure Group	Subnet 192.168.22.0	LAN of Branch B		

	255.255.255.0	
Remote Gateway	Any	Since WAN IP of Branch B gateway is not known in advance, use "Any" to designate the WAN IP of Branch B gateway
Local ID	None	
Remote ID	E-Mail user_b@asus.com.tw	ID of Branch B
Preshared Key	abcd	

VPN Connection Settings											
ID 2: HUB_B 💌 Name			me HUB_B			 Enable 	O Disable	Move	to 2 🗸		
VPN Connection Type				⊙ Site to Site	O Remote Access						
VPN Keep Alive				OEnable	 Dis 	able					
Local Secure Group				Туре	Any	~					
Remote Secure Group				Type	Subne	et 💌					
				Address Subnet Mask	192.10	68.22.0 55.255.0					
Local Gateway				Interface	eth0	~					
Remo	te G	ateway	/	Туре	Any	*					
Local	ID			Туре	None	*					
_	Remote ID			Туре	E-Mai	· ·					
Remo				E-Mail	user_	b@asus.(com.tw				
Key M	lana	gemer	it	Preshared Key 💊	٢						
				IKE I	Propos	sal Setti	ngs				
IKE M	ode			🔘 Main 🛛 🧕	O Main O Aggressive						
Xauth				OEnabled (Disal	bled					
Presh	ared	Key		••••	••••						
IKE Er	noryp	otion/A	uthentication	ALL	*						
Life Ti	ime			3600 sec 🕚	/						
				IPSec	Propo	sal Set	tings				
IPSec	Enc	ryptior	h/Authentication	ALL				*			
Chain	ed A	uthen	tication Header	None OA	H SHA	-1 0	AH MD-5				
Uperation Mode				None w	Trans	ροπ					
Life Ti	ime	P		3600 Sec •	or 7	5000					
				(A		flodify	Delete			Help	
	Remote Access Rules										
		ID	Name	Group Name	Lo	ocal Net	work	Mode	XAUTH	Status	
				Site to S	ite Ac	cess Lis	at Rules				
		ID	Name	Local/Remote N	etwork	¢.	Tunnel End point	4- Key M	gmt. If	PSec Status	
di n	Ē	1	HUB_A	Any 192.168.21.0/24			Any	Presha	red T	unnel Enable	
di i	Ē	2	HUB_B	Any 192.168.22.0/24			Any	Presha	red T	unnel Enable	
Ø	Ē	з	HUB_C	Any 192.168.23.0/24			Any	Presha	red T	unnel Enable	

Configure VPN Rule for the Tunnel between the Headquarter and Branch C

Copyright 2003, ASUSTek Computer, Inc.

Configuration Parameters	Value	Comment
Site-to-Site	Selected	
Enable	Selected	
Tunnel Name	HUB_C	
Local Secure Group	Any	
Remote Secure Group	Subnet 192.168.23.0 255.255.255.0	LAN of Branch C
Remote Gateway	Any	Since WAN IP of Branch C gateway is not known in advance, use "Any" to designate the WAN IP of Branch C gateway
Local ID	None	
Remote ID	E-Mail user_c@asus.com.tw	ID of Branch C
Preshared Key	5678	

VPN Connection Settings										
ID 🛛	3: HUB	_C 🔽	Na	ame HUB_C		📀 Enable 🤇	Disable	Move to 3	~	
VPN Connection Type				⊙ Site to Site	ORemote	e Access				
VPN Keep Alive				○ Enable	📀 Disable	!				
Loca	I Seci	ure Gr	oup	Туре	Any	*				
Remote Secure Group				Type Subnet Address Subnet Mask	Subnet 192.168.23 255.255.26	• 3.0 55.0				
Loca	l Gate	eway		Interface	eth0 💊					
Rem	ote G	atewa	y	Туре	Any	*				
Loca	II ID			Туре	None	*				
Rem	ote IC)		Type E-Mail	E-Mail user_c@a	✓ sus.com.tw				
Key	Mana	gemer	nt	Preshared Key 🔹	*					
				IKE	Proposal S	ettings				
IKE N	Mode 5			O Main (Main Aggressive Dischlod					
Dres	u harec	l Kev		O Enableu						
IKE E	Encrvi	otion/A	uthentication	ALL	~					
Life ⁻	Time			3600 sec 1	~					
				IPSed	: Proposal	Settings				
IPSe	c Enc	ryptior	h/Authentication	ALL			*			
Chai	ned A	luthen	tication Header	⊙None ⊙A	AH SHA-1	⊖ AH MD-5				
Operation Mode				💿 Tunnel 🔘) Transport					
PFS Life	Grou Timo	þ		None V	75000					
Life	nine			3000 800	or / 5000	KByte			Hala	
				A	aa (Modi	Delete			neip	
	Remote Access Rules									
		ID	Name	Group Name	Local	Network	Mode	XAUTH	Status	
				Site to S	Site Acces	s List Rules				
		ID	Name	Local/Remote N	etwork	Tunnel End- point	Key Mg	mt. IPSec	Status	
ø	Ē	1	HUB_A	Any 192.168.21.0/24		Any	Preshare	ed Tunnel	Enable	
Ø	Ē	2	HUB_B	Any 192.168.22.0/24		Any	Preshare	ed Tunnel	Enable	
ø	Ē	3	HUB_C	Any 192.168.23.0/24		Any	Preshare	ed Tunnel	Enable	