HUB AND SPOKE VPN

Release Date: 2005/6/29

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.

Note

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.

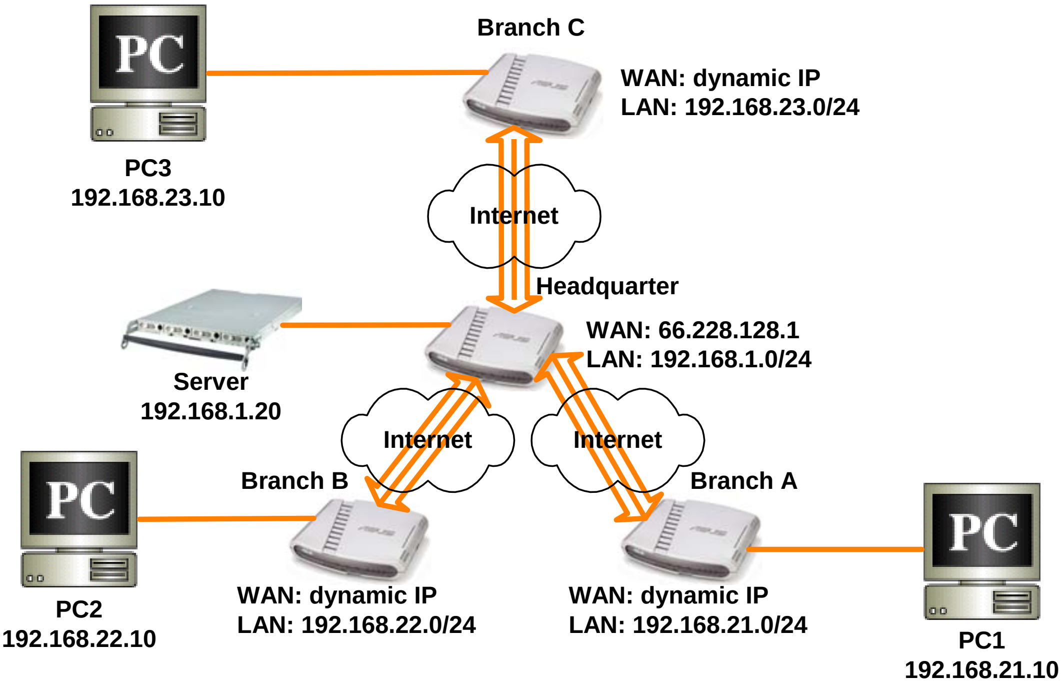


Figure 2.1. Network Toppology Diagram – Dynamic IP for All Branch Offices

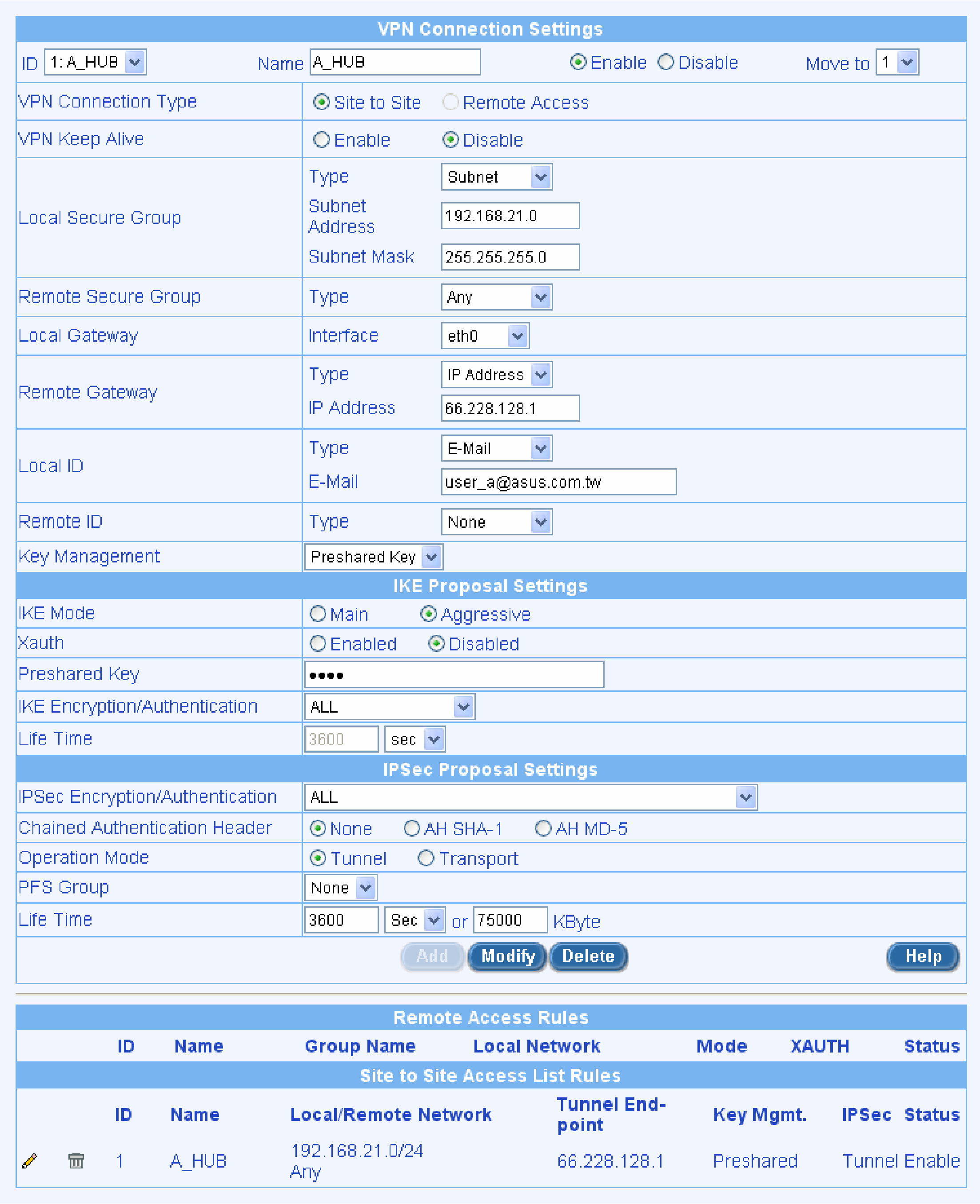
2.2 Setup IPSec VPN for Branch A

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	



VPN Connection Settings

ID 1: A_HUB　Name A_HUB　● Enable ○ Disable　Move to 1

VPN Connection Type	● Site to Site ○ Remote Access	
VPN Keep Alive	○ Enable ● Disable	
Local Secure Group	Type	Subnet
	Subnet Address	192.168.21.0
	Subnet Mask	255.255.255.0
Remote Secure Group	Type	Any
Local Gateway	Interface	eth0
Remote Gateway	Type	IP Address
	IP Address	66.228.128.1
Local ID	Type	E-Mail
	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	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	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 Any	66.228.128.1	Preshared	Tunnel	Enable

2.3 Setup IPSec VPN for Branch B

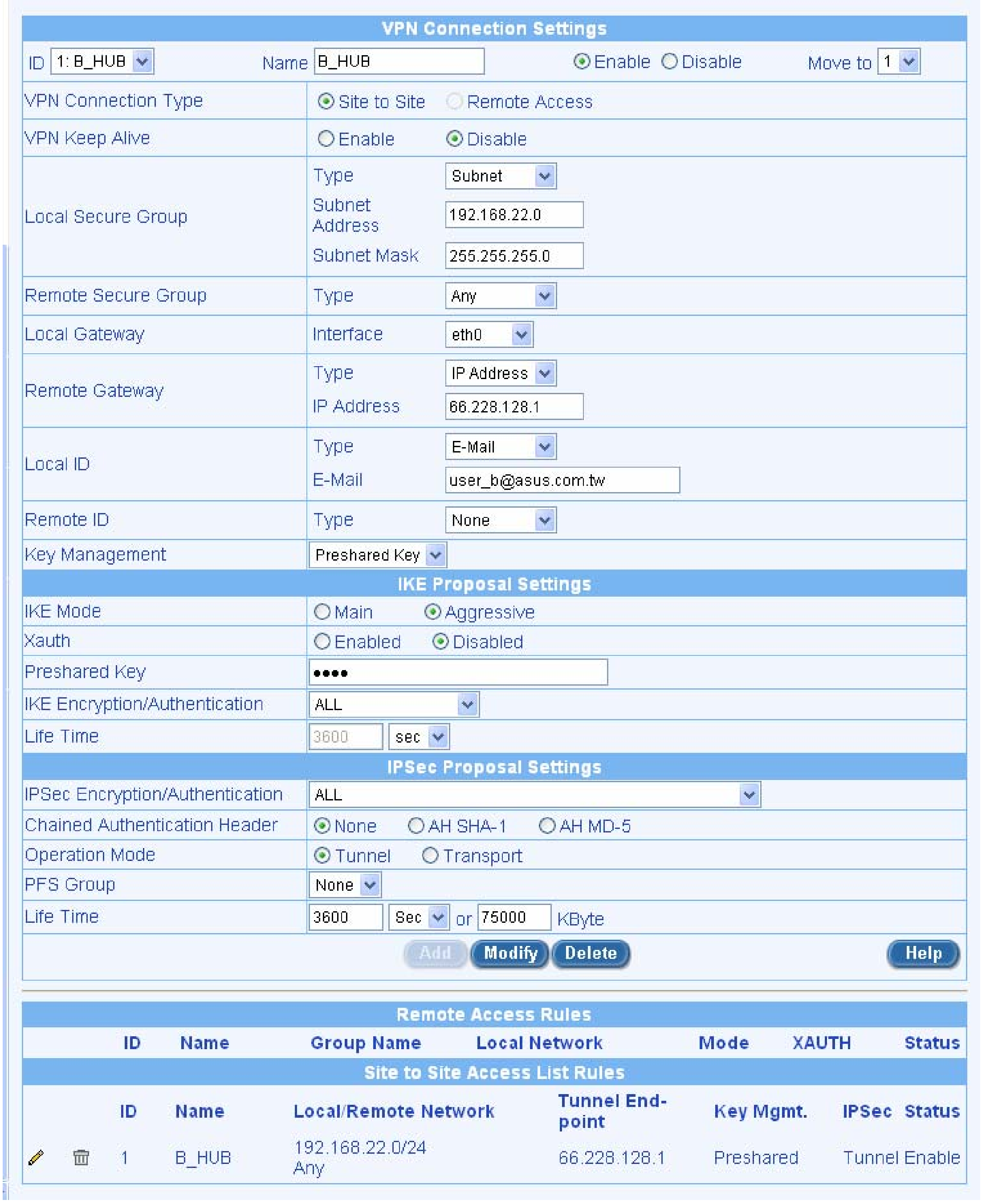
The set up procedure involves:

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	

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 Name B_HUB ● Enable ○ Disable Move to 1

VPN Connection Type	● Site to Site ○ Remote Access	
VPN Keep Alive	○ Enable ● Disable	
Local Secure Group	Type	Subnet
	Subnet Address	192.168.22.0
	Subnet Mask	255.255.255.0
Remote Secure Group	Type	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.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	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	Status

Site to Site Access List Rules

		ID	Name	Local/Remote Network	Tunnel End-point	Key Mgmt.	IPSec	Status
✎	🗑	1	B_HUB	192.168.22.0/24 Any	66.228.128.1	Preshared	Tunnel	Enable

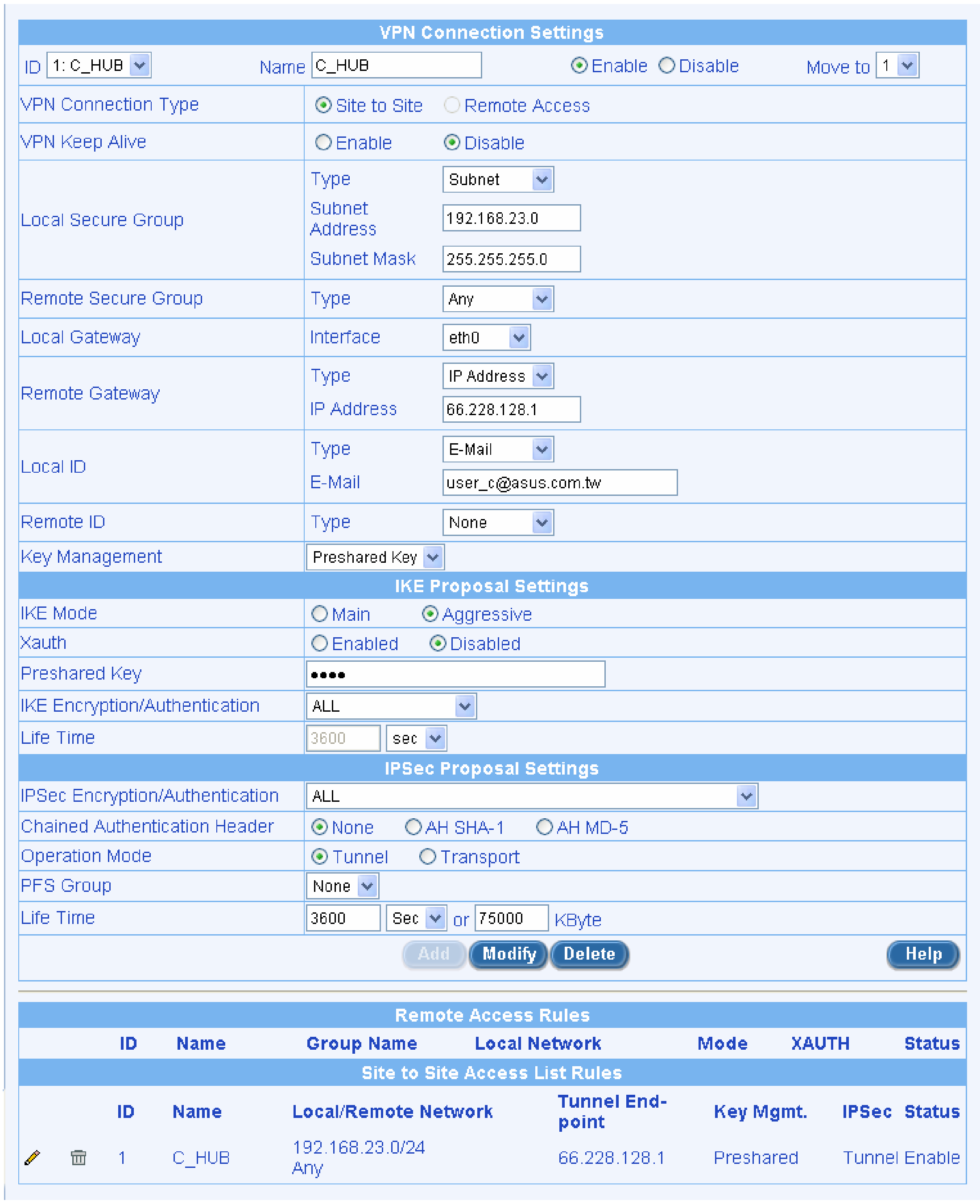
2.4 Setup IPSec VPN for Branch C

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 ○ Disable   Move to 1

VPN Connection Type	● Site to Site ○ Remote Access	
VPN Keep Alive	○ Enable ● Disable	
Local Secure Group	Type	Subnet
	Subnet Address	192.168.23.0
	Subnet Mask	255.255.255.0
Remote Secure Group	Type	Any
Local Gateway	Interface	eth0
Remote Gateway	Type	IP Address
	IP Address	66.228.128.1
Local ID	Type	E-Mail
	E-Mail	user_c@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	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	Status

Site to Site Access List Rules

		ID	Name	Local/Remote Network	Tunnel End-point	Key Mgmt.	IPSec Status
✎	🗑	1	C_HUB	192.168.23.0/24 Any	66.228.128.1	Preshared	Tunnel Enable

2.5 Setup IPSec VPN for the Headquarter

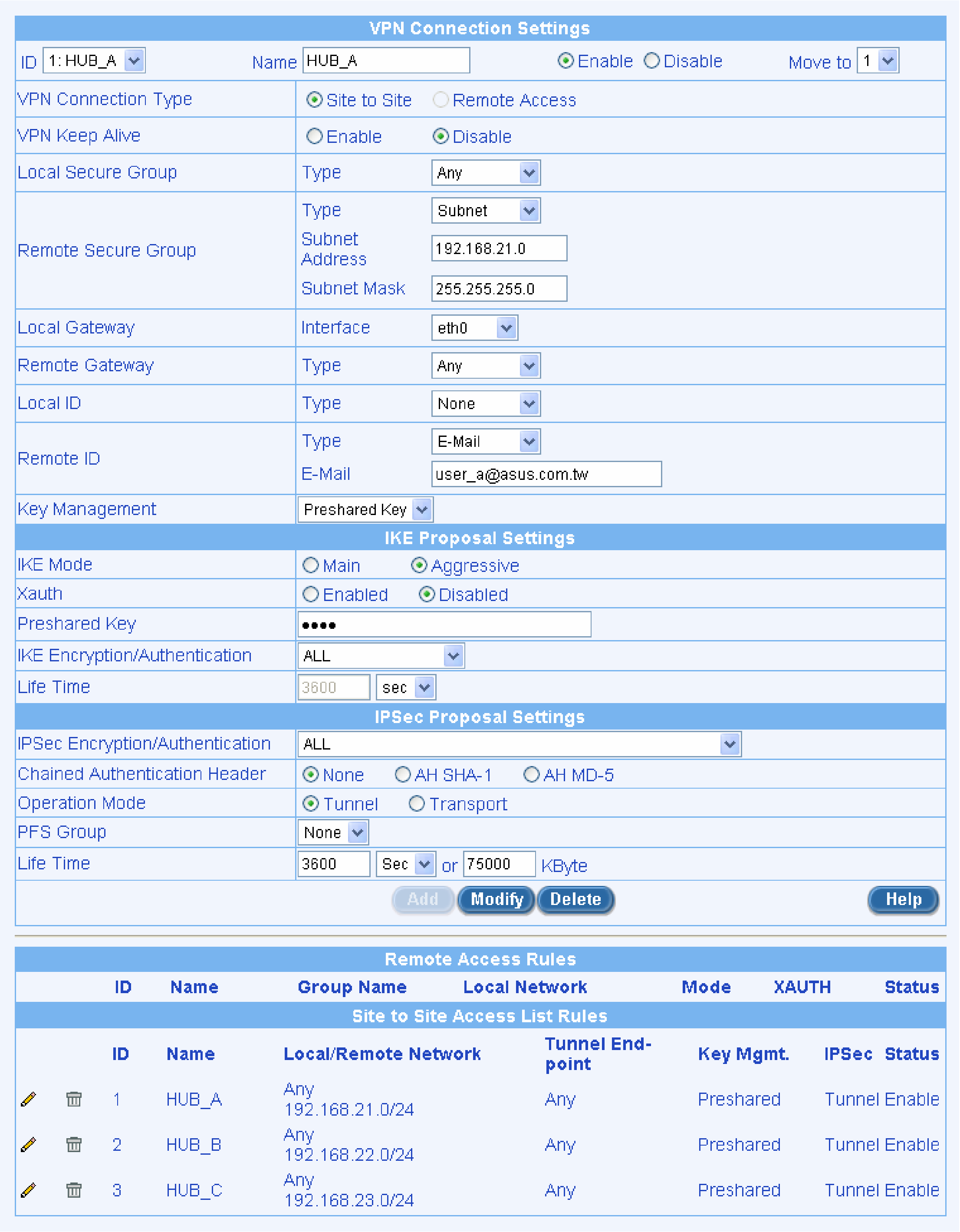
The set up procedure involves:

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 Connection Settings

ID 1: HUB_A	Name HUB_A	● Enable ○ Disable Move to 1
VPN Connection Type	● Site to Site ○ Remote Access	
VPN Keep Alive	○ Enable ● Disable	
Local Secure Group	Type	Any
Remote Secure Group	Type Subnet Address Subnet Mask	Subnet 192.168.21.0 255.255.255.0
Local Gateway	Interface	eth0
Remote Gateway	Type	Any
Local ID	Type	None
Remote ID	Type E-Mail	E-Mail user_a@asus.com.tw
Key Management	Preshared Key	

IKE Proposal Settings

IKE Mode	○ Main ● Aggressive
Xauth	○ 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	Status

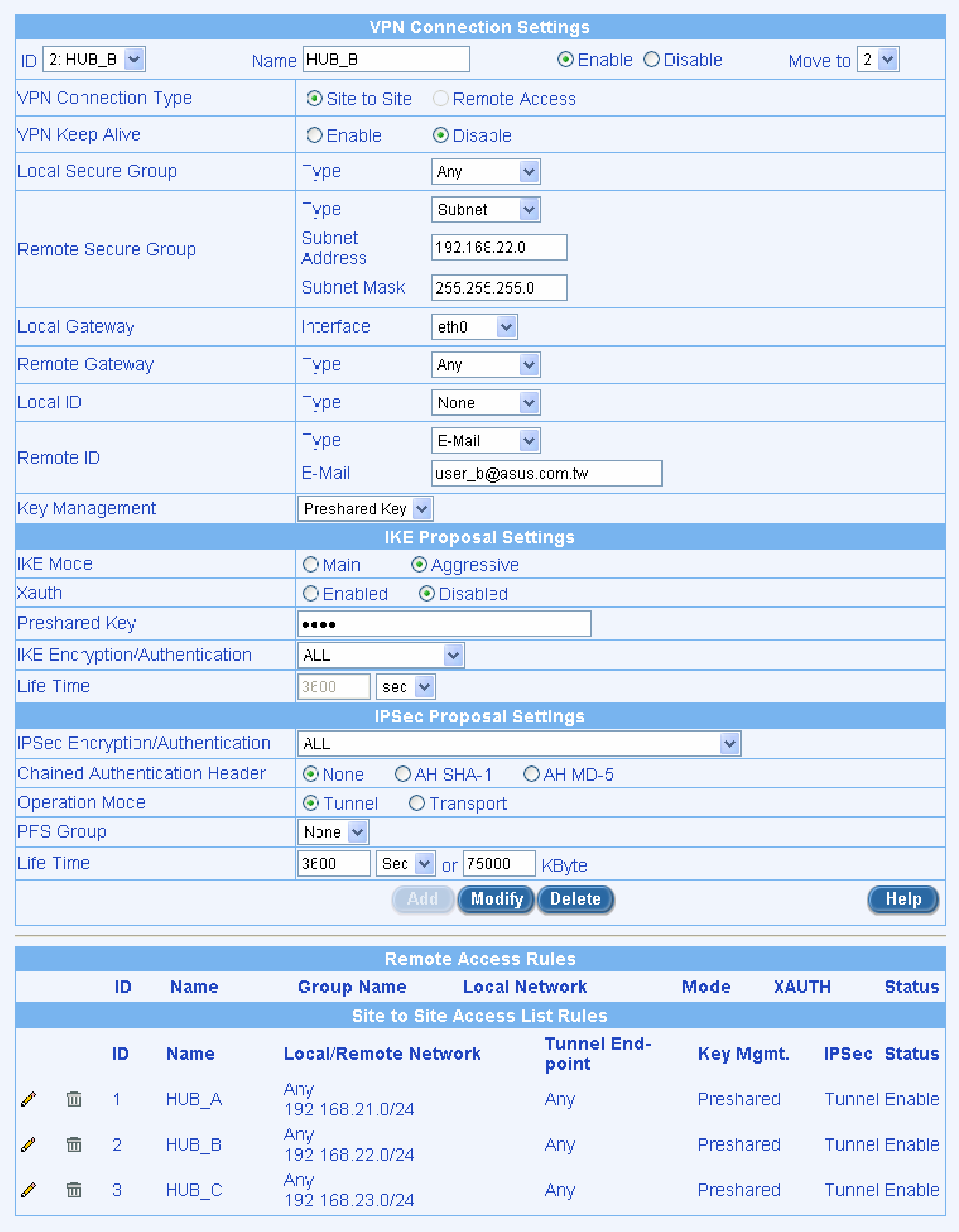
Site to Site Access List Rules

		ID	Name	Local/Remote Network	Tunnel End-point	Key Mgmt.	IPSec	Status
✎	🗑	1	HUB_A	Any 192.168.21.0/24	Any	Preshared	Tunnel	Enable
✎	🗑	2	HUB_B	Any 192.168.22.0/24	Any	Preshared	Tunnel	Enable
✎	🗑	3	HUB_C	Any 192.168.23.0/24	Any	Preshared	Tunnel	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 HUB_B   ● Enable ○ Disable   Move to 2

VPN Connection Type	● Site to Site ○ Remote Access	
VPN Keep Alive	○ Enable ● Disable	
Local Secure Group	Type	Any
Remote Secure Group	Type	Subnet
	Subnet Address	192.168.22.0
	Subnet Mask	255.255.255.0
Local Gateway	Interface	eth0
Remote Gateway	Type	Any
Local ID	Type	None
Remote ID	Type	E-Mail
	E-Mail	user_b@asus.com.tw
Key Management	Preshared Key	

IKE Proposal Settings

IKE Mode	○ Main ● Aggressive
Xauth	○ 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

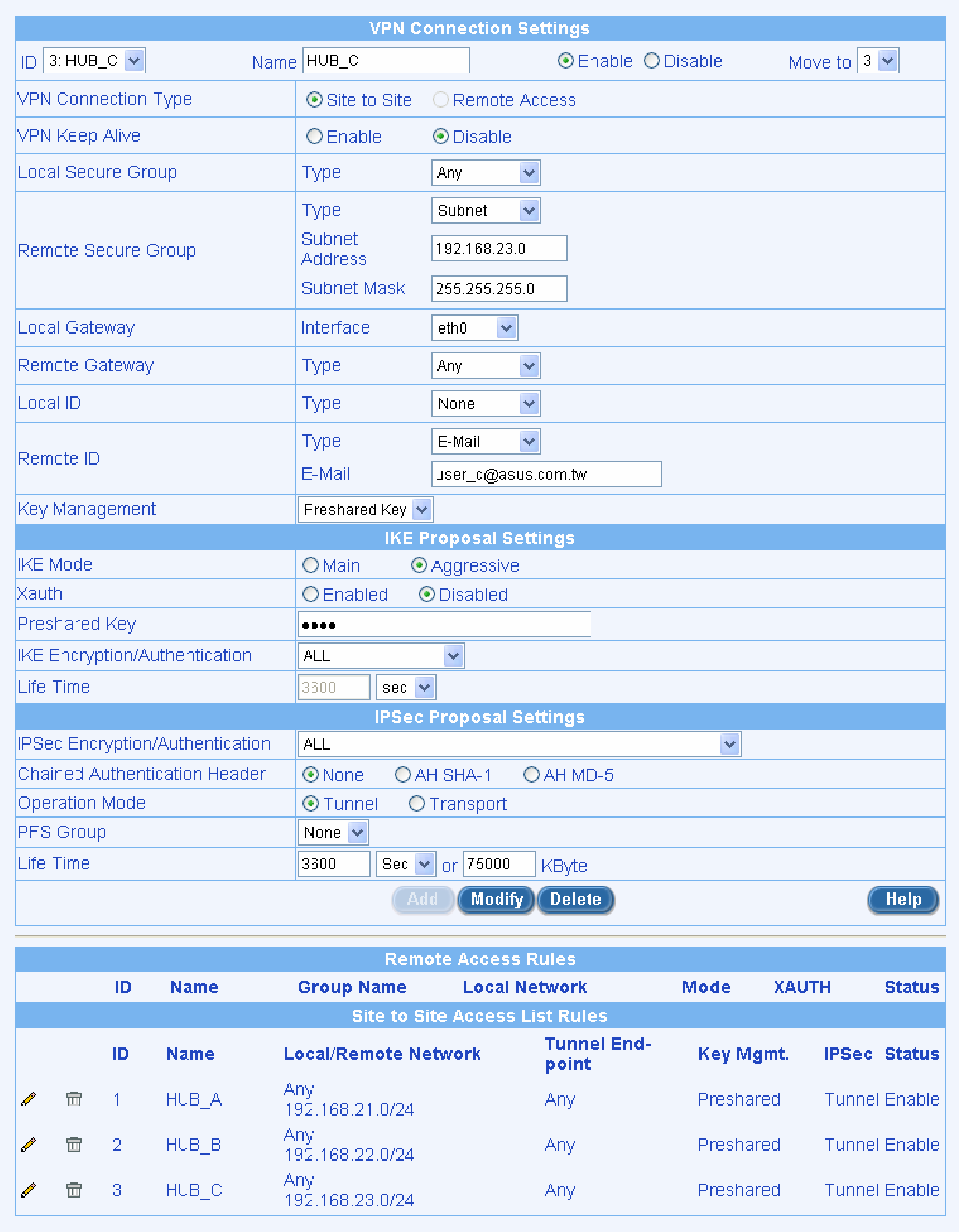
ID	Name	Group Name	Local Network	Mode	XAUTH	Status

Site to Site Access List Rules

		ID	Name	Local/Remote Network	Tunnel End-point	Key Mgmt.	IPSec	Status
✎	🗑	1	HUB_A	Any 192.168.21.0/24	Any	Preshared	Tunnel	Enable
✎	🗑	2	HUB_B	Any 192.168.22.0/24	Any	Preshared	Tunnel	Enable
✎	🗑	3	HUB_C	Any 192.168.23.0/24	Any	Preshared	Tunnel	Enable

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

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 ▾ Name HUB_C ● Enable ○ Disable Move to 3 ▾

VPN Connection Type	● Site to Site ○ Remote Access	
VPN Keep Alive	○ Enable ● Disable	
Local Secure Group	Type	Any ▾
Remote Secure Group	Type	Subnet ▾
	Subnet Address	192.168.23.0
	Subnet Mask	255.255.255.0
Local Gateway	Interface	eth0 ▾
Remote Gateway	Type	Any ▾
Local ID	Type	None ▾
Remote ID	Type	E-Mail ▾
	E-Mail	user_c@asus.com.tw
Key Management	Preshared Key ▾	

IKE Proposal Settings

IKE Mode	○ Main ● Aggressive
Xauth	○ 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

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	HUB_A	Any 192.168.21.0/24	Any	Preshared	Tunnel	Enable
✎	🗑	2	HUB_B	Any 192.168.22.0/24	Any	Preshared	Tunnel	Enable
✎	🗑	3	HUB_C	Any 192.168.23.0/24	Any	Preshared	Tunnel	Enable