

Date: 14/11/2007

Revision Date (6 months max): N/A

Topic / Issue: IPSEC VPN Configuration between Lockdown-SME and IP470VPN

Written By: Scott Young

The following technical article explains the configuration steps required to complete a VPN connection between the Lockdown-SME and the IP470VPN.

This article assumes that you have a pre-configured connection to the internet with both ends having static IP addresses. Configuration of the Lockdown-SME

Note: You must have firmware version v1.25.1 or above to enable VPN features in the Lockdown-SME.

1) Browse to the web management of the Lockdown-SME and click on VPN in the menu on the left hand side. Now select IPSEC Autokey to configure an IPSEC based VPN.



The screenshot displays the web management interface for the Lockdown-SME. The top navigation bar includes "BANDWIDTH MANAGER" and "IPSec Autokey". A sidebar menu on the left lists various configuration options, with "IPSec Autokey" highlighted. The main content area features a table with columns for "Name", "Gateway IP", "Dest. Subnet", "Algorithm", "Status", and "Configure". A "New Entry" button is positioned below the table.

2) Click on New Entry to create a new VPN Tunnel.

3) You will now have to fill out the required sections in the following form:

Enter a Name for your VPN Tunnel. This should be a descriptive name detailing the VPN endpoint.

In the From Source Subnet/Mask section please enter the local IP range of your internal network.

In the To Destination section, for this example we are using static IP addresses at both ends, therefore we will be using Remote Gateway -- Fixed IP. Here you need to enter the WAN IP address of the Remote VPN endpoint.

The Authentication Method used will be Preshare. The preshared key provides a way of authentication between the two devices; this key must be the same at both ends of the VPN tunnel. Enter your key in the space provided

The Encapsulation area determines what encryption and authentication algorithms will be used to communicate between the Lockdown-SME and the IP470VPN.

From the ENC Algorithm drop down box select DES.

From the Auth Algorithm drop down box select MD5.

From the Group drop down box select Group 1.

BANDWIDTH MANAGER **IPsec Autokey**

VPN Auto Keyed Tunnel

Name: Alloy_Test

From Source

Subnet / Mask: 203.33.178.0 / 255.255.255.0

To Destination

Remote Gateway -- Fixed IP: 203.142.137.198

Subnet / Mask: 192.168.0.0 / 255.255.255.0

Remote Gateway -- Dynamic IP

Subnet / Mask: / 255.255.255.0

Remote Client -- Fixed IP or Dynamic IP

Authentication Method: Preshare

Preshared Key: alloytest

Encapsulation

ISAKMP Algorithm

ENC Algorithm: DES

AUTH Algorithm: MD5

Group: GROUP1

IPsec Algorithm

Data Encryption + Authentication

ENC Algorithm: DES

Now check the Data Encryption + Authentication radio button.

From the ENC Algorithm drop down box select DES.

From the Auth Algorithm drop down box select MD5.

Leave the Perfect Forward Secrecy box unchecked this is not needed when used in conjunction with the IP470VPN.

You can change the value of the IPSEC Lifetime value, this determines how long the IPSEC key is used before it is dropped and another key is re-generated.

In the Keep Alive IP section enter an IP address of a device on the remote network that can be used to keep the VPN connection alive.

Aggressive Mode and GRE/IPSEC will not be used in this configuration.

If you have a preconfigured QoS Policy or Schedule configured these can also be applied to your VPN.

Tick the Show Remote Network Neighbourhood check box. This allows NetBIOS traffic to pass through your VPN connection.

BANDWIDTH MANAGER **IPsec Autokey**

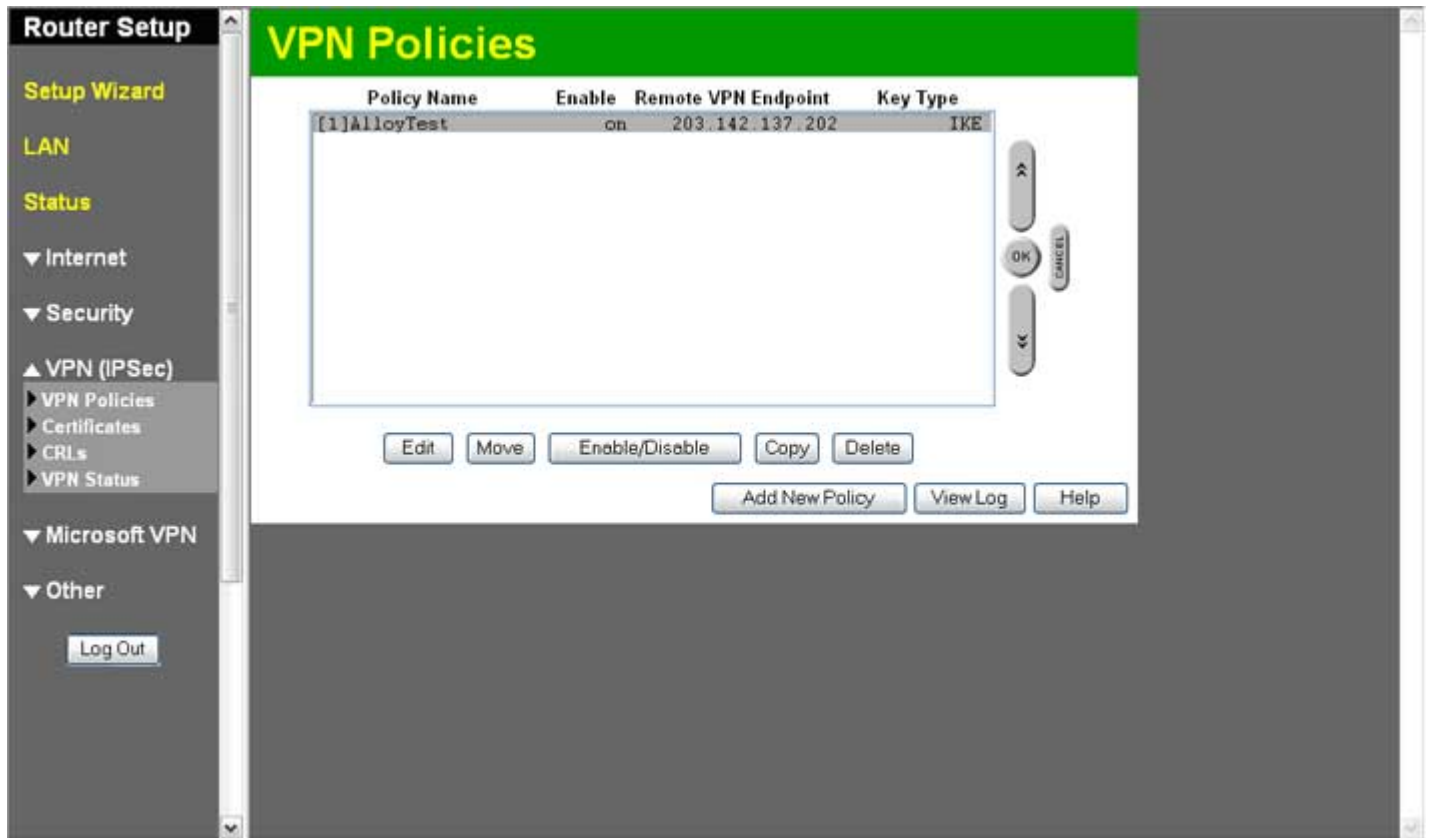
System	Group	GROUP1
Interface	IPsec Algorithm	
Address	<input checked="" type="radio"/> Data Encryption + Authentication	
Service	ENC Algorithm	DES
Schedule	AUTH Algorithm	MD5
QoS	<input type="radio"/> Authentication Only	
Authentication	<input type="checkbox"/> Perfect Forward Secrecy	
Content Filtering	IPsec Lifetime	28800 Seconds
Virtual Server	Keep alive IP :	203.142.137.198
Policy	<input type="checkbox"/> Aggressive mode	
VPN	My ID	<input type="text"/> (ex: 172.16.0.1 or @my_id.domain)
IPsec Autokey	Peer ID	<input type="text"/> (ex: 172.16.0.2 or @peer_id.domain)
PPTP Server	<input type="checkbox"/> GRE/IPsec	
PPTP Client	GRE Local IP	<input type="text"/> (ex: 10.0.0.1)
Log	GRE Remote IP	<input type="text"/> (ex: 10.0.0.2)
Alarm	Schedule	None
Accounting Report	QoS	None
Statistics	<input checked="" type="checkbox"/> Show remote Network Neighborhood	
Status		

OK Cancel

Now click the OK button to save your IPSEC VPN configuration.

Configuration of the IP470VPN

1) Browse to the configuration of the IP470VPN and click on VPN (IPSEC) in the menu on the left. Now select VPN Policies to configure an IPSEC based VPN.



2) Click on Add New Policy to create your VPN Policy.

3) Click on Setup Screen and fill out the following form:

Enter a descriptive Name for your VPN Configuration.

Check the Enable Policy check box and also check the Allow Netbios Traffic check box. This allows Netbios traffic to pass through your VPN Tunnel.

In the Remote VPN Endpoint section check the Fixed IP radio button and enter the IP Address of the remote VPN endpoint.

The Local IP Addresses section is used to determine the local LAN IP address range used on your internal network. From the drop down box select Subnet Address and enter your local IP Range and Subnet Mask in the space provided.

The Remote IP Addresses section is used to determine the Remote LAN IP address range used on your remote internal network. From the drop down box select Subnet Address and enter your Remote IP Range and Subnet Mask in the space provided.

The Authentication and Encryption section determines what encryption and authentication algorithms will be used to communicate between the Lockdown-SME and the IP470VPN.

Tick the ESP Encryption check box and select DES from the drop down box.

Tick the ESP Authentication check box and select MD5 from the drop down box.

Router Setup

VPN Policy Definition

Name: AlloyTest Enable Policy
 Allow NetBIOS traffic

Remote VPN endpoint Dynamic IP
 Fixed IP: 203.142.137.202
 Domain Name: _____

Local IP addresses
 Type: Subnet address IP address: 192.168.0.0 ~ 0
 Subnet Mask: 255.255.255.0

Remote IP addresses
 Type: Subnet address IP address: 203.33.178.0 ~ 0
 Subnet Mask: 255.255.255.0

Authentication & Encryption
 AH Authentication MD5
 ESP Encryption DES Key Size: n/a (AES only)
 ESP Authentication MD5
 Manual Key Exchange
 IKE (Internet Key Exchange)
 Direction: Both Directions
 Local Identity Type: WAN IP Address
 Local Identity Data: 203.142.137.198

Check the IKE radio button and next to Direction select Both Directions.

The Local Identity Type will be WAN IP Address; this will not allow you to enter anything in the Local Identity Data field as it will be filled in automatically.

The Remote Identity Type will be Remote WAN IP, this will not allow you to enter anything in the Remote Identity Data field as it will be filled in automatically.

The Authentication type that will be used is Preshared Key, select the Preshared Key radio button and enter the preshared key in the space provided.

The Authentication Algorithm to be used will be MD5 and the Encryption Algorithm used will be DES

The Exchange Mode that will be used is Main Mode.

You can also specify the IKE SA Life Time and IPSEC SA Life Time, this determines how long the IPSEC and IKE key is used before it is dropped and another key is re-generated.

In the Keep Alive IP section enter an IP address of a device on the remote network that can be used to keep the VPN connection alive.

The DH Group can be set accordingly with the configuration at the other end, for this example we will be using Group 1.

The IKE and IPSEC PFS (Preferred Forward Secrecy) will not be used in this configuration, therefore these will be set to Disabled.

Router Setup

- Setup Wizard
- LAN
- Status
- Internet
- Security
- VPN (IPSec)
 - VPN Policies
 - Certificates
 - CRLs
 - VPN Status
- Microsoft VPN
- Other
 - Log Out

ESP Encryption DES Key Size: n/a (AES only)
 ESP Authentication MD5
 Manual Key Exchange
 IKE (Internet Key Exchange)

Direction: Both Directions
 Local Identity Type: WAN IP Address
 Local Identity Data: 203.142.137.198
 Remote Identity Type: Remote WAN IP
 Remote Identity Data: 203.142.137.202
 Authentication:

- RSA Signature (requires certificate)
- Pre-shared Key: alloytest

 Authentication Algorithm: MD5

Encryption: DES Key Size: n/a (AES only)
 Exchange Mode: Main Mode
 IKE SA Life Time: 180 (secs)
 IKE Keep Alive Ping IP Address: 203.142.137.202
 IPsec SA Life Time: 300 (secs)
 DH Group: Group 1 (768 Bit)
 IKE PFS: Disabled
 IPsec PFS: None

Your VPN should now be setup correctly, to establish a connection between both devices you can either ping an IP Address on the opposite side of the VPN or you can manually establish the connection via the Lockdown-SME Web Management.

Router Setup

- Setup Wizard
- LAN
- Status
- Internet
- Security
- VPN (IPSec)
 - VPN Policies
 - Certificates
 - CRLs
 - VPN Status
- Microsoft VPN
- Other
 - Log Out

VPN Status

Current VPN SAs

Policy Name	SPI	Type	VPN Endpoint	Data Transferred
AlloyTest	7320effc	ESP	203.142.137.202	420
INAlloyTest	daa2997f	ESP	203.142.137.198	420

System
Interface
Address
Service
Schedule
QoS
Authentication
Content Filtering
Virtual Server
Policy
VPN
IPSec Autokey
PPTP Server
PPTP Client
Log
Alarm
Accounting Report
Statistics
Status

Name	Gateway IP	Dest. Subnet	Algorithm	Status	Configure
Alloy_Test	203.142.137.198	192.168.0.0	DES_HMAC_MD5	Connect	Disconnect Modify Remove

[New Entry](#)

Summary:
(If required)