

This document provides information about using IP Security Protocol (IPSec), Internet Key Exchange (IKE) technology with the MB8000.

This is a case study on how to configure an IPSec VPN tunnel on MB8000.

This chapter includes the following sections:

1. How IPSec Works
2. Internet Key Exchange (IKE)
3. Configuring IPSec

## How IPSec Works

IPSec provides authentication and encryption services to protect unauthorized viewing or modification of data within your network or as it is transferred over an unprotected network, such as the public Internet.

Two different security protocols are included within the IPSec standard:

**Encapsulated Security Protocol (ESP)**—Provides authentication, encryption, and anti-replay services.

**Authentication Header (AH)**—Provides authentication and anti-replay services. This protocol has largely been superseded by ESP.

IPSec in MB8000 can be configured to work in Tunnel mode:

This is the normal way in which IPSec is implemented between one MB8000 and a VPN server that are connected over an unsecured network, such as the public Internet.

The main task of IPSec is to allow the exchange of private information over an insecure connection. IPSec uses encryption to protect information from interception or eavesdropping. However, to use encryption efficiently, both parties should share a secret that is used for both encryption and decrypting of the information.

IPSec operates in two phases to allow the confidential exchange of a shared secret:

**Phase 1**, which handles the negotiation of security parameters required to establish a secure channel between two IPSec peers. Phase 1 is generally implemented through the Internet Key Exchange (IKE) protocol. If the remote IPSec peer cannot do IKE, you can use manual configuration with pre-shared keys to complete Phase 1.

**Phase 2**, which uses the secure tunnel established in Phase 1 to exchange the security parameters required to actually transmit user data.

The secure tunnels used in both phases of IPSec are based on security associations (SAs) used at each IPSec end point. SAs describe the security parameters, such as the type of authentication and encryption that both end points agree to use.

## Internet Key Exchange (IKE)

This section describes the Internet Key Exchange (IKE) protocol and how it works with IPSec to make VPN more scalable.

IKE is a protocol used by IPSec for completion of Phase 1. IKE negotiates and assigns SAs for each IPSec peer, which provides a secure channel for the negotiation of the IPSec SAs in Phase 2. IKE provides the following benefits:

- Eliminates the need to manually specify all the IPSec security parameters at both peers
- Lets you specify a lifetime for the IPSec SAs
- Allows encryption keys to change during IPSec sessions
- Allows IPSec to provide anti-replay services
- Allows dynamic authentication of peers

IKE negotiations have to be protected, so each IKE negotiation begins by each peer agreeing on a common (shared) IKE policy. This policy states the security parameters that will be used to protect subsequent IKE negotiations. After the two peers agree upon a policy, the security parameters of the policy are identified by an SA established at each peer, and these SAs apply to all subsequent IKE traffic during the negotiation.

There are five parameters to define in each IKE policy. These parameters apply to the IKE negotiations when the IKE SA is established. The following table provides the five IKE policy parameters and their permitted values.

**IKE Policy Keywords**

<b>Keyword</b>	<b>Meaning</b>	<b>Description</b>
DES	56-bit DES-CBC	Specifies the symmetric encryption algorithm used to protect user data transmitted between two IPsec peers.
3DES	168-bit Triple DES	
SHA	SHA-1 (HMAC variant)	Specifies the hash algorithm used to ensure data integrity. The default is SHA-1. MD5 has a smaller digest and is considered to be slightly faster than SHA-1. There has been a demonstrated successful (but extremely difficult) attack against MD5; however, the HMAC variant used by IKE prevents this attack.
MD5	MD5 (HMAC variant)	
768	Group 1 (768-bit Diffie-Hellman)	Specifies the Diffie-Hellman group identifier, which is used by the two IPsec peers to derive a shared secret without transmitting it to each other. The default, Group 1 (768-bit Diffie-Hellman) requires less CPU time to execute but is less secure than Group 2 (1024-bit Diffie-Hellman).
1024	Group 2 (1024-bit Diffie-Hellman)	
	any number of seconds	Specifies the SA lifetime. <b>The default is 86,400 seconds or 24 hours.</b> As a general rule, a shorter the lifetime (up to a point) provides more secure IKE negotiations. However, with longer lifetimes, future IPsec security associations can be set up more quickly
	Pre-shared keys	Pre-shared keys do not scale well with a growing network but are easier to set up in a small network

You can create multiple IKE policies, each with a different combination of parameter values. If you do not configure any policies, VPN function of your MB8000 will not work.

When the IKE negotiation begins, the peer that initiates the negotiation will send all its policies to the remote peer, and the remote peer will try to find a match.

A match is made when both policies from the two peers contain the same encryption, hash, authentication, and Diffie-Hellman parameter values, and when the remote

peer's policy specifies a lifetime less than or equal to the lifetime in the policy being compared. If the lifetimes are not identical, the shorter lifetime—from the remote peer's policy—will be used.

If no acceptable match is found, IKE refuses negotiation and IPSec will not be established. If a match is found, IKE will complete negotiation, and IPSec security associations will be created.

## Configuring IPSec

1. Log in to MB8000. MB8000 is set for its default LAN address of `http://172.16.0.1` with its default user name of **public** and default password of **public**
2. Click on the VPN Settings link on the left side of the main menu.

Advanced

- Password
- Encryption
- Radius Authentication
- Radius Accounting
- Filters
- Web Portal
- IP Port Forwarding
- Link Integrity
- Dynamic DNS
- VPN**
- Greeting
- GPS
- Static Route
- PPP

SetUp — VPN — VPN Configuration

VPN Status:

Establish Automatically:

DPD Status:

DPD Interval:

DPD Timeout:

Click the first button to establish VPN connection manually, and click the second button to disconnect VPN connection manually. View the log to find the result.

VPN Table:

	Local net	Remote net	Remote gw	P1 mode	P1 Enc Alg	P1 Hash Alg	Status
<input checked="" type="checkbox"/>	171.16.0.0	192.168.0.0	124.42.52.4	Main	3DES	MD5	Enable

- **VPN Status.** Indicates whether VPN function is enabled or not.
- **Establish Automatically.** When enabled, VPN tunnel will be established automatically after PPP is opened.
- **DPD Status.** Indicates whether DPD function is enabled or not.
- **DPD Interval.** The interval of DPD.

- **DPD Timeout.** The timeout of DPD.
3. Click Add to add a VPN tunnel
  4. Or click the radio button of an available VPN tunnel , then click Edit.

**VPN Configuration**

Mode: *Tunnel*

Tunnel Status:

Local Subnet Address:

Local Subnet Mask:

Remote Subnet Address:

Remote Subnet Mask:

Remote Gateway Address:

---

**Phase 1 proposal(Authentication)**

Mode:

Encryption Algorithm:

Hash Algorithm:

DH Key Group:

Lifetime:  (Seconds)

Authmethod:

Preshared Key:

---

**Phase 2 proposal(SA/Key Exchange)**

ESP:

AH:

Encryption Algorithm:

Hmac Algorithm:

PFS Key Group:

Lifetime:  (Seconds)

Lifebyte:  (KBytes)

- **Tunnel Status.** Select **Enable** to enable the tunnel.
- **Local subnet Address and local subnet Mask.** The Local network is the computer(s) on your LAN that can access the tunnel. These fields are read-only.
- **Remote subnet Address and remote subnet Mask .** The Remote network is the computer (s) on the remote end of the tunnel that can access the tunnel.
- **Remote Gateway Address.** The Remote Gateway is the VPN device on the remote end of the VPN tunnel. Enter the IP Address of the VPN device at the other end of the tunnel. **The remote VPN device can be another VPN Server,**

or a computer with VPN client software that supports IPsec. Make sure that you have entered the IP Address correctly, or the connection cannot be made. Remember, this is NOT the IP Address of the local VPN Router, but the IP Address of the remote device with which you wish to communicate.

## Phase 1

Phase 1 is used to create a security association (SA), often called the IKE SA. After Phase 1 is completed, Phase 2 is used to create one or more IPsec SAs, which are then used to key IPsec sessions.

- **Mode.** There are two modes: Main and Aggressive, and they exchange the same IKE payloads in different sequences. Main mode is more common; however, some people prefer Aggressive mode because it is faster. Main mode is for normal usage and includes more authentication requirements than Aggressive mode. Main mode is recommended because it is more secure.
- **Encryption Algorithm.** Select the length of the key used to encrypt/decrypt ESP packets. There are two choices: DES and 3DES. 3DES is recommended because it is more secure.
- **Hash Algorithm.** Select the method used to authenticate ESP packets. There are two choices: MD5 and SHA. SHA is recommended because it is more secure.
- **DH Key Group.** There are two Diffie-Hellman Groups to choose from: 768-bit and 1024-bit. Diffie-Hellman refers to a cryptographic technique that uses public and private keys for encryption and decryption.
- **LifeTime.** In the Key Lifetime field, you may optionally select to have the key expire at the end of a time period of your choosing. Enter the number of seconds you'd like the key to be used until a re-key negotiation between each endpoint is completed.
- **Auth method.**
- **Preshared Key.**

## Phase 2

- **Encryption Algorithm.** Select the length of the key used to encrypt/decrypt ESP packets. There are two choices: DES and 3DES. 3DES is recommended because it is more secure.
- **Hmac Algorithm.** Select the method used to authenticate ESP packets. There are two choices: MD5 and SHA. SHA is recommended because it is more secure.
- **PFS Key Group.** There are two Diffie-Hellman Groups to choose from: 768-bit and 1024-bit. Diffie-Hellman refers to a cryptographic technique that uses public and private keys for encryption and decryption.
- **LifeTime.** In the Key Lifetime field, you may optionally select to have the key expire at the end of a time period of your choosing. Enter the number of seconds you'd like the key to be used until a re-key negotiation between each endpoint is completed.
- **LifeBye.**