Default Encryption Settings for the Microsoft L2TP/IPSec Virtual Private Network Client

Summary

The following list contains the default encryption settings for the Microsoft L2TP/IPSec virtual private network (VPN) client for earlier version clients:

- Data Encryption Standard
- Secure Hash Algorithm
- Diffie-hellman Medium
- Transport Mode
- Encapsulating Security Payload

The client does not support the following settings:

- Tunnel mode
- AH (Authentication Header)

These values are hard-coded in the client and you cannot change them.

More Information

Data Encryption Standard

Data Encryption Standard (3DES) provides confidentiality. 3DES is the most secure of the DES combinations, and has a bit slower performance. 3DES processes each block three times, using a unique key each time.

Secure Hash Algorithm

Secure Hash Algorithm 1(SHA1), with a 160-bit key, provides data integrity.

Diffie-Hellman Medium

Diffie-Hellman groups determine the length of the base prime numbers that are used during the key exchange. The strength of any key derived depends in part on the strength of the Diffie-Hellman group on which the prime numbers are based.

Group 2 (medium) is stronger than Group 1 (low). Group 1 provides 768 bits of keying material, and Group 2 provides 1,024 bits. If mismatched groups are specified on each peer, negotiation does not succeed. You cannot switch the group during the negotiation.

A larger group results in more entropy and therefore a key that is harder to break.

Transport Mode

There are two modes of operation for IPSec:

- Transport mode - In transport mode, only the payload of the message is encrypted.
- Tunnel mode (not supported) - In tunnel mode, the payload, the header, and the routing information are all encrypted.

IPSec Security Protocols

Encapsulating Security Payload

Encapsulating Security Payload (ESP) provides confidentiality, authentication, integrity, and anti-replay. ESP does not ordinarily sign the whole packet unless the packet is being tunneled. Ordinarily, only the data is protected, not the IP header. ESP does not provide integrity for the IP header (addressing).

Authentication Header (Not Supported)

Authentication Header (AH) provides authentication, integrity, and anti-replay for the whole packet (both the IP header and the data carried in the packet). AH signs the whole packet. It does not encrypt the data, so it does not provide confidentiality. You can read the data, but you cannot modify it. AH uses HMAC algorithms to sign the packet.

References

For additional information, click the article numbers below to view the articles in the Microsoft Knowledge Base:

325035 Limitations and Compatibility Issues of Microsoft L2TP/IPSec VPN

325032 Using the Microsoft L2TP/IPSec

VPN Client with Windows 98, Windows Millennium Edition, and Windows NT 4.0

325033 Configuring Microsoft L2TP/IPSec VPN for Earlier Clients

325034 Troubleshooting Microsoft L2TP/IPSec VPN Client Connection

Poslední aktualizace: 17. 4. 2018