|  |  |  |  |
| --- | --- | --- | --- |
| **Command** | **Keyword** | **Meaning** | **Description** |
| **crypto isakmp policy authentication** | rsa-sig | A digital certificate with keys generated by the RSA signatures algorithm | Specifies the authentication method the security appliance uses to establish the identity of each IPsec peer. |
| crack | Challenge/Response for Authenticated Cryptographic Keys | CRACK provides strong mutual authentication when the client authenticates using a legacy method such as RADIUS and the server uses public key authentication. |
| pre-share  (default) | Preshared keys | Preshared keys do not scale well with a growing network but are easier to set up in a small network. |
| **crypto isakmp policy encryption** | des  3des (default) | 56-bit DES-CBC  168-bit Triple DES | Specifies the symmetric encryption algorithm that protects data transmitted between two IPsec peers. The default is 168-bit Triple DES. |
| aes aes-192 aes-256 |  | The Advanced Encryption Standard supports key lengths of 128, 192, 256 bits. |
| **crypto isakmp policy group** | 1 | Group 1 (768-bit) | Specifies the Diffie-Hellman group identifier, which the two IPsec peers use to derive a shared secret without transmitting it to each other.  With the exception of Group 7, the lower the Diffie-Hellman group no., the less CPU time it requires to execute. The higher the Diffie-Hellman group no., the greater the security.  Cisco VPN Client Version 3.x or higher requires a minimum of Group 2. (If you configure DH Group 1, the Cisco VPN Client cannot connect.)  AES support is available on security appliances licensed for VPN-3DES only. To support the large key sizes required by AES, ISAKMP negotiation should use Diffie-Hellman (DH) Group 5.  Designed for devices with low processing power, such as PDAs and mobile telephones, Group 7 provides the greatest security. The Certicom Movian Client requires Group 7. |
| 2 (default) | Group 2 (1024-bit) |
| 5 | Group 5 (1536-bit) |
| 7 | Group 7 (Elliptical curve field size is 163 bits.) |
| **Table 27-1 ISAKMP Policy Keywords for CLI Commands** | | | |

Pre-Shared Key (PSK) is a client authentication method that uses a string of 64 hexadecimal digits, or as a passphrase of 8 to 63 printable ASCII characters, to generate unique encryption keys for each wireless client.

**ISAKMP is the negotiation protocol that lets two hosts agree on how to build an IPsec security association (SA)**

| Transform Type | Transform | Description |
| --- | --- | --- |
| **AH Transform**(*Pick only one.*) | **ah-md5-hmac** | AH with the MD5 (Message Digest 5) (an HMAC variant) authentication algorithm. (No longer recommended). |
| **ah-sha-hmac** | AH with the SHA (Secure Hash Algorithm) (an HMAC variant) authentication algorithm.  A transform set combination of AH and ESP is not supported in Cisco IOS XE releases. |
| **ESP Encryption Transform**(*Pick only one.*) | **esp-aes** | ESP with the 128-bit Advanced Encryption Standard (AES) encryption algorithm. |
| **esp-gcm**  **esp-gmac** | The **esp-gcm**and **esp-gmac**transforms are ESPs with either a 128-bit or a 256-bit encryption algorithm. The default for either of these transforms is 128 bits.  Both **esp-gcm**and **esp-gmac**transforms cannot be configured together with any other ESP transform within the same crypto IPsec transform set using the **crypto ipsec transform-set**command.  The esp-gcm and esp-gmac combinations are not supported on the Cisco ASR 1001 routers with the following ESPs:   * ESP-5 * ESP-10 * ESP-20 * ESP-40 |
| **esp-aes 192** | ESP with the 192-bit AES encryption algorithm. |
| **esp-aes 256** | ESP with the 256-bit AES encryption algorithm. |
|  | **esp-des** | ESP with the 56-bit Data Encryption Standard (DES) encryption algorithm. (No longer recommended).   |  |  | | --- | --- | | **Note** | When using DES, 3DES, or GMAC transforms on Cisco ASR 1001-X and Cisco ASR 1002-X routers with ESP-100 or ESP-200, there might be a 30% performance degradation compared to AES and GCM. | |
| **esp-3des** | ESP with the 168-bit DES encryption algorithm (3DES or Triple DES). (No longer recommended). |
| **esp-null** | Null encryption algorithm. |
|  |  |
| **ESP Authentication Transform**(*Pick only one.*) | **esp-md5-hmac** | ESP with the MD5 (HMAC variant) authentication algorithm. (No longer recommended). |
| **esp-sha-hmac** | ESP with the SHA (HMAC variant) authentication algorithm. |
| **Table 1. Allowed Transform Combinations** | | |

**Hashed Message Authentication Codes** (HMAC) The fundamental hash algorithms used by IPSec are the cryptographically secure Message Digest 5 (MD5) and Secure Hash Algorithm 1 (SHA-1) hash functions.

A crypto map performs two primary functions: • Selects data flows that need security processing. • Defines the policy for these flows and the crypto peer to which that traffic needs to go. A crypto map is applied to an interface.

When configuring a IPSec VPN tunnel, it is recommended to enable PFS, or Perfect Forward Secrecy if both side of the VPN devices support the technology. It provides a more secure VPN tunnel.  it performs an authenticated Diffe-Hellman exchange and making sure the Pre-share Key (PSK) matches

This is the lifetime of the keys that the tunnel uses to encrypt data