--

**1) Configuración de IKE.** “Internet Key Exchange” es un protocolo que define el método

de intercambio de claves sobre IP en una primera fase de negociación segura. Está formado por una cabecera de autenticación (AH) o una cabecera de autenticación más cifrado (Encapsulating Security Payload o ESP).

conf t

crypto isakmp policy **10**

encr **AES**

authentication pre-share

group **5** *(Diffie-Hellman grupo 5 – clave de 1536 bits)*

lifetime **900** *(tiempo de vida en segundos)*

exit

**Notas técnicas**:

• crypto isakmp policy **10**: *este comando crea la política ISAKMP número 10. Puede crear varias políticas, por ejemplo 7, 8, 9 con una configuración diferente. Los routers que participan en la negociación de la Fase 1 buscan la coincidencia de políticas ISAKMP con la lista de políticas una por una. Si alguna política coincide, la negociación de IPSec pasa a la Fase 2.*

• encr **AES**: *se utilizará el algoritmo AES para la fase 1.*

• authentication pre-share: *el método de autenticación es una clave pre-compartida.*

• group **5**: *el grupo Diffie-Hellman que se utilizará es el 5 (grupo de 1536 bits).*

*Los grupos Diffie-Hellman (DH) determinan la fuerza de la clave usada en el proceso de intercambio de claves. Los miembros de grupos más altos (DF 14, 15, 19 y 20)son más seguros, pero se necesita más tiempo para computar la clave. Ambos puntos en un intercambio de VPN deben usar el mismo grupo DH, que es negociado durante la Fase 1 del proceso de negociación de IPSec. Es ahí donde los dos puntos forman un canal seguro y autenticado que pueden usar para comunicarse.*

• lifetime **900**: *tiempo de vida en segundos.*

**Definición de una clave simétrica con el otro extremo del túnel:**

crypto isakmp key **cisco** address **10.2.0.2**

(La contraseña de la fase 1 es “cisco” y la dirección IP remota es 10.2.0.2)

**2) Configuración de IPSec modo túnel**

crypto ipsec transform-set 50 ah-sha-hmac esp-3des

(Para listar las otras opciones de autenticación y encriptación utilice el comando *crypto ipsec transform-set* ***50*** *?*)