

Creating Site-to-Site VPNs with Pre-Shared Keys

Documentation:

1. Document your IKE Phase 1 negotiation criteria (example below)
 - Encryption algorithm: AES-128
 - Hashing: SHA-1
 - Authentication: pre-shared
 - Key exchange: Diffie-Hellman Group 2
2. Document your IPsec (IKE Phase 2) negotiation criteria (example below)
 - Encryption algorithm: esp-aes 128
 - Authentication: esp-sha-hmac

Configuring IKE Phase 1:

1. Enable ISAKMP: `Router(config)#crypto isakmp enable`
2. Create ISAKMP Policy: `Router(config)#crypto isakmp policy <1-10000>`
 - `Router(config)#crypto isakmp policy 100`
 - `Router(config-isakmp)#encryption aes 128`
 - `Router(config-isakmp)#authentication pre-share`
 - `Router(config-isakmp)#group 2`
 - `Router(config-isakmp)#hash sha`
3. Configure ISAKMP Identity: `Router(config)#crypto isakmp identity <address/hostname>`
4. Configure pre-shared keys: `Router(config)#crypto isakmp key <key> address <remote_ip>`

Configuring IKE Phase 2:

1. Create transform sets: `Router(config)#crypto ipsec transform-set <name> <methods>`
 - `Router(config)#crypto ipsec transform-set JEREMY esp-aes 128 esp-sha-hmac`
2. (optional) Configure IPsec lifetime: `Router(config)#crypto ipsec <seconds/kilobytes> <value>`
3. Create mirrored ACLs defining traffic to be encrypted and the traffic expected to be received encrypted
4. Set up IPsec crypto-map: `Router(config)#crypto isakmp map <name> <seq> ipsec-isakmp`
 - `Router(config)#crypto map MAP 100 ipsec-isakmp`
 - `Router(config-crypto-map)#match address <acl>`
 - `Router(config-crypto-map)#set peer <remote_ip>`
 - `Router(config-crypto-map)#set pfs <group1/2/5>`
 - `Router(config-crypto-map)#set transform-set <set>`

Verify:

- `show crypto isakmp policy`
- `show crypto ipsec transform-set`
- `show crypto ipsec sa`
- `show crypto map`
- `debug crypto isakmp`
- `debug crypto ipsec`