

Implementing Virtual Private Networks

IKE Phase1

negotiate one bidirectional IKE Security Association (SA) (Aggressive Mode / Main Mode)

Authentication

1. ISAKMP aktivieren (Internet Security Association and Key Management Protocol)

```
ROUTER(config)#crypto isakmp enable
```

2. ISAKMP-Policy

```
ROUTER(config)#crypto isakmp policy 1
ROUTER(config-isakmp)#authentication pre-share
ROUTER(config-isakmp)#encryption aes 256
ROUTER(config-isakmp)#group 5
ROUTER(config-isakmp)#hash sha
ROUTER(config-isakmp)#lifetime 3600
```

priority
rsa-sig | pre-share | rsa-encr
des | 3des | aes 128 | aes 192 | aes 256
 Diffie-Hellman group 5 (1 | 2 | 5 | 14 | 15 | 16)
sha | md5
 eine Stunde

3. Pre-Shared Key and username

```
ROUTER(config)#crypto isakmp key XXXX address 1.2.3.4
```

IP-Adresse des Gegenübers ist username

Diagnose

```
ROUTER#debug crypto isakmp
ROUTER#show crypto isakmp policy
ROUTER#show crypto isakmp sa
```

IKE Phase2

negotiate two unidirectional IPsec Security Associations (SAs)

1. Crypto-ACL: Interesting Traffic

```
ROUTER(config)#access-list 101 permit ip QUELLE ZIEL
```

2. Transform-Set: confidentiality / integrity-algorithms

```
ROUTER(config)#crypto ipsec transform-set MYSET esp-aes 256 esp-sha-hmac
```

3. Crypto-Map: Verknüpfung von Peer address, Transform-set und Crypto-ACL

```
ROUTER(config)#crypto map MYMAP 10 ipsec-isakmp
ROUTER(config-crypto-map)#match address 101
ROUTER(config-crypto-map)#set peer 1.2.3.4
ROUTER(config-crypto-map)#set transform-set MYSET
```

eine map kann mehrere Sequenznummern haben

4. Interface

```
ROUTER(config)#interface S2/0
ROUTER(config-if)#crypto map MYMAP
```

Diagnose

```
ROUTER#debug crypto ipsec
ROUTER#show crypto ipsec transform-set
ROUTER#show crypto map
ROUTER#show crypto ipsec sa
ROUTER#show crypto engine connection active
ROUTER#show crypto session
```