

1. ISAKMP-szabályobjektum létrehozása

```
Router(config)#crypto isakmp policy 1
```

a. Diffie-Hellman számítás modulusának meghatározása

```
Router(config-isakmp)#group 2 (1-es csoport 768 bit, 2-es csoport 1024 bit)
```

b. Kivonatoló algoritmus meghatározása

```
Router(config-isakmp)#hash md5
```

c. Biztonsági kapcsolat élettartamának meghatározása másodpercben

```
Router(config-isakmp)#lifetime 1000
```

d. A hitelesítéshez használatos kulcs megadása

```
Router(config-isakmp)#authentication pre-share (RSA aláírás)
```

e. A hitelesítéshez szükséges algoritmus megadása

```
Router(config-isakmp)#encryption aes 128
```

f. Kilépés ISAKMP szabályobjektum megadásából

```
Router(config-isakmp)#exit
```

2. A ISAKMP-kulcs kiválasztása

```
Router(config)#crypto isakmp key KULCS address [távoli végpont IP-cím]
```

3. IPSec paramétereinek beállítása

a. Kiterjesztett ACL létrehozása

```
Router(config)#access-list 101 permit ip [forrás-IP maszk][cél-IP maszk]
```

b. IPSec átalakítások létrehozása

```
Router(config)#crypto ipsec transform-set ELNEVEZÉS ah-md5-hmac esp-des
```

c. Titkosítási leképezés létrehozása

```
Router(config)#crypto map LEKÉPEZÉS_NÉV 10 ipsec-isakmp
```

```
Router(config-crypto-map)#set peer [távoli végpont IP-cím]
```

```
Router(config-crypto-map)#set session-key lifetime seconds 4000
```

```
Router(config-crypto-map)#set transform-set ELNEVEZÉS
```

```
Router(config-crypto-map)#match address 101 (az ACL száma)
```

d. Titkosítási leképezés interfészhez rendelése (KIMENŐ INTERFÉSZ!!!)

```
Router(config)#interface Serial S0/0/0
```

```
Router(config-if)#crypto map LEKÉPEZÉS_NÉV
```

VPN ellenőrzésére szolgáló parancsok

```
Router#show crypto ipsec sa
```

```
Router#show crypto ipsec transform-set
```

```
Router#show crypto isakmp policy
```

```
Router#show crypto isakmp sa
```

```
Router#show crypto map
```