

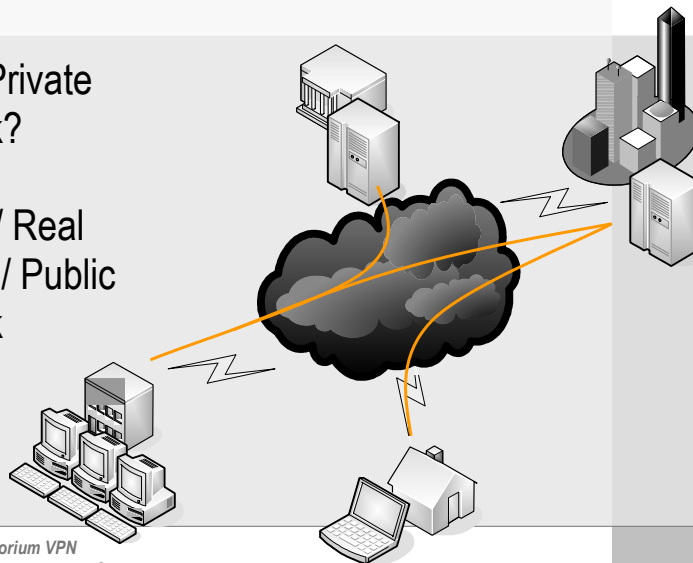
# Laboratorium Wirtualne sieci prywatne

Igor Margasiński  
Instytut Telekomunikacji, Politechnika Warszawska

OINS, 24 kwietnia 2008

## VPN

- Virtual Private Network?
- **Virtual** / Real
- **Private** / Public
- Network



Igor Margasiński - *Laboratorium VPN*

2.

## Plan prezentacji

- Podstawowe polecenia
- Weryfikacja konfiguracji
- Budowa tunelu
- Scenariusz laboratorium

## IKE: parametry polityki

■Parameter	■Strong	■Stronger
■Encryption algorithm	■DES	■3DES or AES
■Hash algorithm	■MD5	■SHA-1
■Authentication method	■Pre-shared	■RSA encryption ■RSA signature
■Key exchange	■DH Group 1	■DH Group 2 ■DH Group 5
■IKE SA lifetime	■86,400 seconds	■Less than 86,400 seconds

## Przekształcenia IPsec

```
RouterA(config)# crypto ipsec transform-set
  transform-set-name ?
ah-md5-hmac    AH-HMAC-MD5 transform
ah-sha-hmac    AH-HMAC-SHA transform
comp-lzs       IP compression using LZS compression algorithm
esp-3des       ESP transform using 3DES(EDE) cipher (168 bits)
esp-aes        ESP transform using AES cipher
esp-des        ESP transform using DES cipher (56 bits)
esp-md5-hmac   ESP transform using HMAC-MD5 auth
esp-null       ESP transform w/o cipher
esp-seal       ESP transform using SEAL cipher (160 bits)
esp-sha-hmac   ESP transform using HMAC-SHA auth
```

Igor Margasiński - *Laboratorium VPN*

5.

## Weryfikacja konfiguracji

```
show running-config
```

- polityki IPsec

```
show crypto isakmp policy
```

- polityki IKE

```
RouterA# show crypto isakmp policy
Default protection suite
  encryption algorithm:  DES - Data Encryption Standard (56 bit keys)
  hash algorithm:        Secure Hash Standard
  authentication method: Rivest-Shamir-Adleman Signature
  Diffie-Hellman Group:  #1 (768 bit)
  lifetime:               86400 seconds, no volume limit
```

Igor Margasiński - *Laboratorium VPN*

6.

## Weryfikacja konfiguracji cd

```
show crypto map
```

```
RouterA# show crypto map
Crypto Map "mymap" 10 ipsec-isakmp
Peer = 172.30.2.2
Extended IP access list 102
  access-list 102 permit ip host 172.30.1.2 host 172.30.2.2
Current peer: 172.30.2.2
Security association lifetime: 4608000 kilobytes/3600 seconds
PFS (Y/N): N
Transform sets={ mine, }
```

## Weryfikacja konfiguracji cd

```
show crypto ipsec transform-set
```

**Przekształcenia kryptograficzne**

```
RouterA# show crypto ipsec transform-set mine
Transform set mine: { esp-des }
will negotiate = { Tunnel, },
```

## Konfiguracja przekształceń kryptograficznych

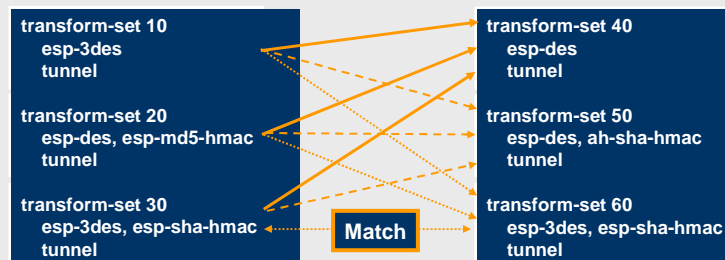
```
router(config)#
```

```
crypto ipsec transform-set transform-set-name  
transform1 [transform2 [transform3]]  
router(cfg-crypto-trans)#
```

```
RouterA(config)# crypto ipsec transform-set MINE  
esp-des esp-md5-hmac
```

- Przekształcenia IPSec mające wdrażać politykę

## Negocjacja polityk

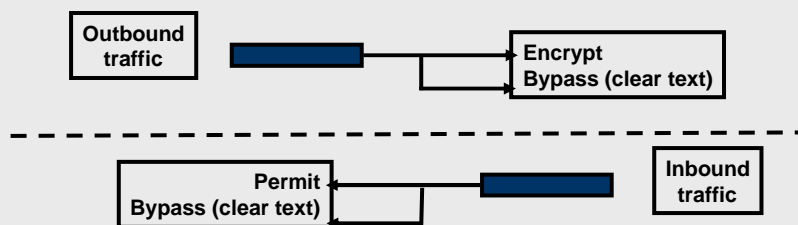


## Czas życia

```
router(config)#  
crypto ipsec security-association lifetime  
  {seconds seconds | kilobytes kilobytes}
```

```
RouterA(config)# crypto ipsec security-association  
lifetime seconds 86400
```

## Wskazanie ruchu do ochrony – *Crypto ACLs*



## Łączenie wszystkiego razem – *Crypto Maps*

- Wyodrębniony ruch do ochrony
- (Crypto ACLs)
- Gdzie ruch chroniony ma być wysyłany
- Skąd ruch chroniony ma być wysyłany
- Parametry IPsec
- Czy SA negocjowane przez IKE

## Łączenie wszystkiego razem – *Crypto Maps cd*

```
router(config)#
```

```
crypto map map-name seq-num ipsec-manual
```

```
crypto map map-name seq-num ipsec-isakmp  
[dynamic dynamic-map-name]
```

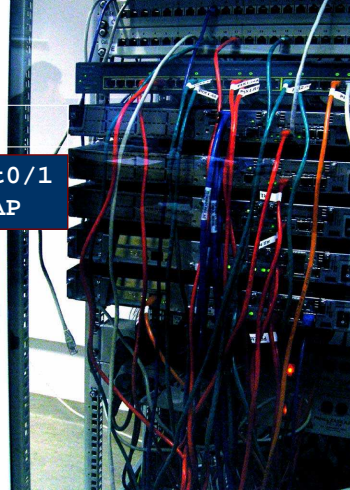
```
RouterA(config)# crypto map MYMAP 110 ipsec-isakmp
```

```
RouterA(config)# crypto map MYMAP 110 ipsec-isakmp  
RouterA(config-crypto-map)# match address 110  
RouterA(config-crypto-map)# set peer 172.30.2.2  
RouterA(config-crypto-map)# set peer 172.30.3.2  
RouterA(config-crypto-map)# set pfs group1  
RouterA(config-crypto-map)# set transform-set MINE  
RouterA(config-crypto-map)# set security-association lifetime  
seconds 86400
```

## Przypisanie Crypto Map

```
router(config-if)#  
crypto map map-name
```

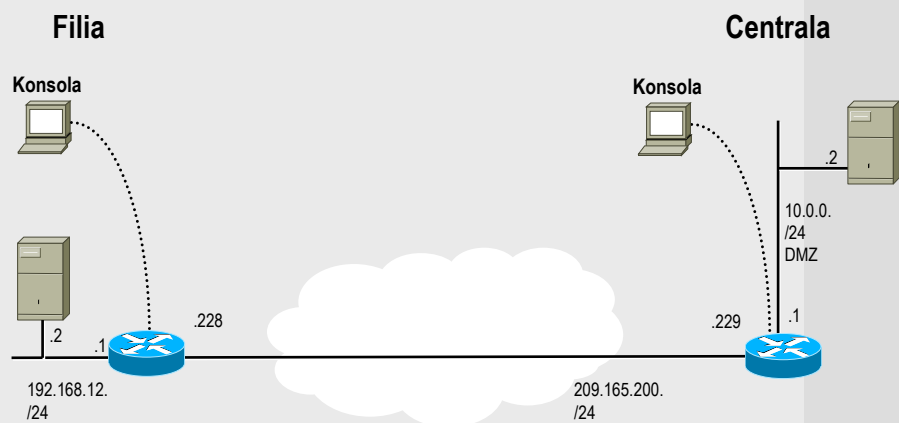
```
RouterA(config)# interface ethernet0/1  
RouterA(config-if)# crypto map MYMAP
```



Igor Margasiński - *Laboratorium VPN*

15.

## Scenariusz laboratorium



Igor Margasiński - *Laboratorium VPN*

16.

**Koniec**

Igor Margasiński  
Instytut Telekomunikacji, Politechnika Warszawska

