

The background of the slide features a large, faint watermark of the seal of the Politecnico di Torino. The seal is circular and contains the text "POLITECNICO DI TORINO" around the perimeter. In the center, there is a depiction of a building with a dome and a figure holding a staff, surrounded by a laurel wreath.

Configuring IPsec on Cisco Routers

Mario Baldi

Politecnico di Torino
(Technical University of Torino)

<http://staff.polito.it/mario.baldi>

Nota di Copyright

This set of transparencies, hereinafter referred to as slides, is protected by copyright laws and provisions of International Treaties. The title and copyright regarding the slides (including, but not limited to, each and every image, photography, animation, video, audio, music and text) are property of the authors specified on page 1.

The slides may be reproduced and used freely by research institutes, schools and Universities for non-profit, institutional purposes. In such cases, no authorization is requested.

Any total or partial use or reproduction (including, but not limited to, reproduction on magnetic media, computer networks, and printed reproduction) is forbidden, unless explicitly authorized by the authors by means of written license.

Information included in these slides is deemed as accurate at the date of publication. Such information is supplied for merely educational purposes and may not be used in designing systems, products, networks, etc. In any case, these slides are subject to changes without any previous notice. The authors do not assume any responsibility for the contents of these slides (including, but not limited to, accuracy, completeness, enforceability, updated-ness of information hereinafter provided).

In any case, accordance with information hereinafter included must not be declared.

In any case, this copyright notice must never be removed and must be reported even in partial uses.

IPsec Configuration Steps

- Encryption and authentication algorithms and parameters
- Encapsulation mode
- Key negotiation
- Secure traffic selection
- Remote tunnel end-point
- Interface on which to apply
- Security association lifespan

Encryption and authentication

```
# crypto ipsec transform-set name  
  TS1 [TS2 [TS3]]
```

→ Enters crypto transform configuration mode

→ Sample *TS_i* values:

→ ah-md5-hmac

→ esp-des

→ esp-md5-hmac

→ Not any combination is allowed

Encapsulation Mode

```
# mode [tunnel | transport]
```

- **Crypto transform configuration mode command**
- **Only for traffic for which the router is the IPsec tunnel endpoint**

Key Negotiation

```
# crypto map name num [ipsec-  
manual | ipsec-isakmp]
```

→ Enters crypto map configuration mode

→ ipsec-manual

→ Secret shared keys

→ Manually configured

→ ipsec-isakmp

→ IKE negotiation is deployed

AH Key Configuration

```
# set session-key {inbound |  
outbound} ah spi key
```

- Crypto map configuration mode command
- Specifies key used for
 - Verification (inbound)
 - Authentication (outbound)

ESP Key Configuration

```
# set session-key {inbound |  
outbound} esp spi cipher e-key  
[authenticator a-key]
```

→ Crypto map configuration mode

→ Specifies key used for

→ Encryption (*e-key*)

→ Authentication (*a-key*)

ISAKMP Negotiation Policy

```
# crypto isakmp policy priority
```

→ Enter ISAKMP configuration mode

→ If other policies do exist and can be used, the one with highest priority is applied

ISAKMP Negotiation Policy

```
# encr {des|3des}
```

→ Encryption algorithm

```
# hash {sha|md5}
```

→ Hash algorithm

```
# authentication {rsa-sig|rsa-  
encr|pre-share}
```

→ Authentication method

→ ISAKMP configuration mode

ISAKMP Shared Key

```
# crypto isakmp key a_key address  
an_address
```

→ *an_address*: remote end of IPsec tunnel

→ ISAKMP configuration mode

Security Options

set transform-set *name*

- Crypto map configuration mode command
- Specifies which of the previously defined encryption and authentication options to use

Secure Traffic Selection

match address *list-num*

- Crypto map configuration mode command
- Only traffic matching access list *list-num* is secured
- One security association is created for each rule of the access list
 - Only one rule is allowed when key negotiation is not used

Remote Tunnel End-Point

set peer *device*

→ Crypto map configuration mode command

→ *device* can be a name or address

Dynamic Parameters

```
# crypto dynamic-map name num
```

→ Enters crypto map configuration mode

→ IKE negotiation must be deployed

Dynamic Parameters

- Remote tunnel end-point specification (`set peer`) optional
- Secure traffic selection (`match address`) is optional
 - Traffic filter provided by remote end-point
 - If specified must match remote end-point's

Interface Specification

`crypto map name`

→ Interface configuration mode command

→ Tunnel interface should be created to implement an IPsec tunnel

Security Association Lifespan

```
# crypto ipsec security-  
association lifetime {seconds  
sec / kilobytes kb}
```

→ Global configuration mode

→ IKE re-negotiation takes place before expiration

→ Whichever of the two limits is reached first

Security Association Lifespan

```
# set security-association  
lifetime {seconds sec |  
kilobytes kb}
```

- Crypto map configuration mode
- Refers to a specific security association