



IPSec

Internet Protocol Security

Mario Baldi

Synchrodyne Networks, Inc.

mbaldi[at]synchrodyne.com





Nota di Copyright



Questo insieme di trasparenze (detto nel seguito slide) è protetto dalle leggi sul copyright e dalle disposizioni dei trattati internazionali. Il titolo ed i copyright relativi alle slide (ivi inclusi, ma non limitatamente, ogni immagine, fotografia, animazione, video, audio, musica e testo) sono di proprietà degli autori indicati a pag. 1.



Le slide possono essere riprodotte ed utilizzate liberamente dagli istituti di ricerca, scolastici ed universitari afferenti al Ministero della Pubblica Istruzione e al Ministero dell'Università e Ricerca Scientifica e Tecnologica, per scopi istituzionali, non a fine di lucro. In tal caso non è richiesta alcuna autorizzazione.

Ogni altra utilizzazione o riproduzione (ivi incluse, ma non limitatamente, le riproduzioni su supporti magnetici, su reti di calcolatori e stampate) in toto o in parte è vietata, se non esplicitamente autorizzata per iscritto, a priori, da parte degli autori.

L'informazione contenuta in queste slide è ritenuta essere accurata alla data della pubblicazione. Essa è fornita per scopi meramente didattici e non per essere utilizzata in progetti di impianti, prodotti, reti, ecc. In ogni caso essa è soggetta a cambiamenti senza preavviso. Gli autori non assumono alcuna responsabilità per il contenuto di queste slide (ivi incluse, ma non limitatamente, la correttezza, completezza, applicabilità, aggiornamento dell'informazione).


In ogni caso non può essere dichiarata conformità all'informazione contenuta in queste slide.

In ogni caso questa nota di copyright non deve mai essere rimossa e deve essere riportata anche in utilizzi parziali.





Overview

- **Application layer security**
 - **Security e-mail**
 - **S/MIME**
 - **DNS security extensions**
 - **SSH (Secure SHell): secure telnet**
 - **Transport layer security**
 - **SSL (Secure Socket Layer)**
 - **Network layer Security**
 - **IPSec**
 - **Protection of IP, TCP, and UDP headers**
 - **Authentication of IP, TCP, and UDP headers**
- 





Problemi di sicurezza

Privacy



Autenticazione

■ IPSec

- Privacy
- Integrità
- Authentication
- Tunneling

■ IKE (Internet Key Exchange)

- Key management - gestione delle chiavi di cifratura
 - Le chiavi vengono cambiate periodicamente
- Gli estremi dei tunnel sono certificati da una Certification Authority

Trasparente per gli utenti















IPSec and IKE

IPSec supports

- manual (out-of-band) key exchange
- IKE

Ingredients:

- Diffie-Hellman key exchanges
 - Public key cryptography to sign key exchanges
 - Guarantees for identities of the two parties
 - Digital certificates to validate public keys
 - DES (Data Encryption Standard) to encrypt data
- 
-
- 
-
- 
-
- 
-
- 
-
- 
-
- 





Security Association (SA)

- Agreements that enable data exchange
- An exchange providing authentication and privacy requires a separate SA for each

An SA includes

- Session keys
- IP address of each endpoint
 - It can be a subnet prefix
- IP address of each IPSec gateway
- Expiration of session keys
 - Upon session keys expiration a new Security Association is to be created





IKE (Internet Key Exchange)

- Means to agree upon
 - Protocols
 - Algorithms
 - Encryption
 - DES
 - 3DES
 - RC5
 - Cast
 - Authentication: message digest
 - MD5
 - SHA1
 - Keys
 - Shared secret
 - Communicated off-line
 - Digital certificates



IKE (Internet Key Exchange)

- Authentication of the other communicating party
- Management of keys agreed upon
 - Session keys are changed regularly
 - One shared pair of session keys per communicating direction
 - one for data encryption
 - one for authentication





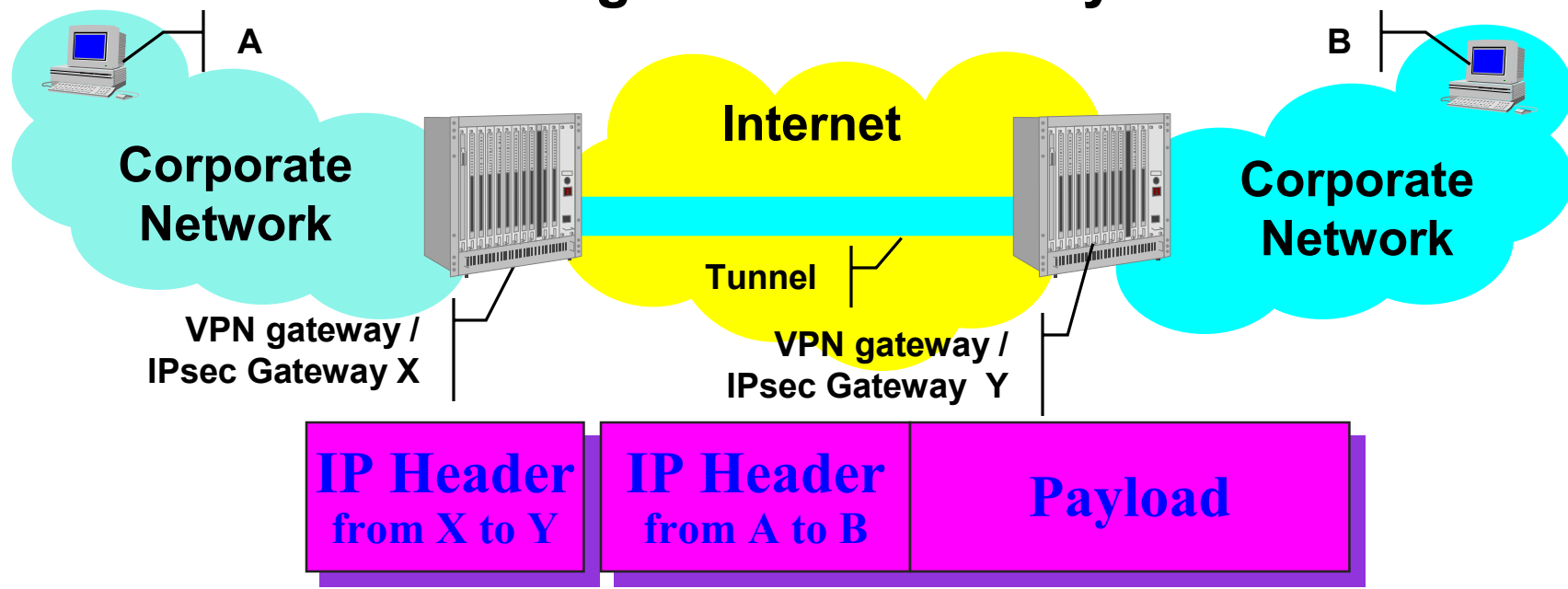
Implementation

- Client implementation
- Gateway implementation
 - Software: on firewall or router
 - Hardware: special purpose box
- Algorithm independence



(IPsec) Tunneling VPN

- A and B are enterprise addresses
 - they do not have to satisfy the public system requirements
- Tunneling enables operation
- IPsec tunneling ensures security



Transport Mode Encapsulation

- Comunicazione tra terminale e terminale
- Le informazioni tra l'intestazione ESP (Encapsulation Security Payload) e il trailer è cifrata
 - Security Parameter Index (SPI)
 - Puntatore nel SA database → tipo di cifratura
- ESP trailer: autenticazione
 - Message authentication code (MAC)
 - Dal trasporto (TCP/UDP) al MAC (escluso)



Transport Mode Encapsulation

- Authentication header
 - SPI
 - Con e senza ESP
 - MAC sull'intero pacchetto
 - no TTL, ToS, informazioni di frammentazione, ecc.

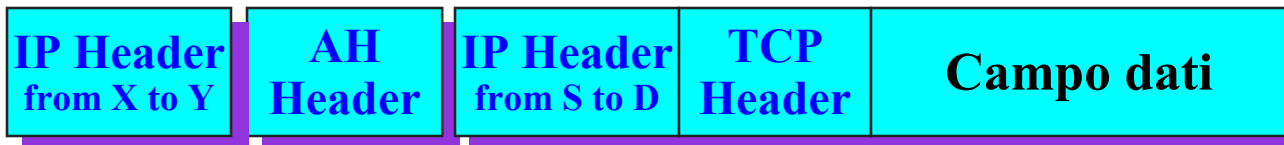


■ Autenticato

▨ Cifrato

Tunnel Mode Encapsulation

Comunicazioni tra il Gateway (X) e il gateway (Y)

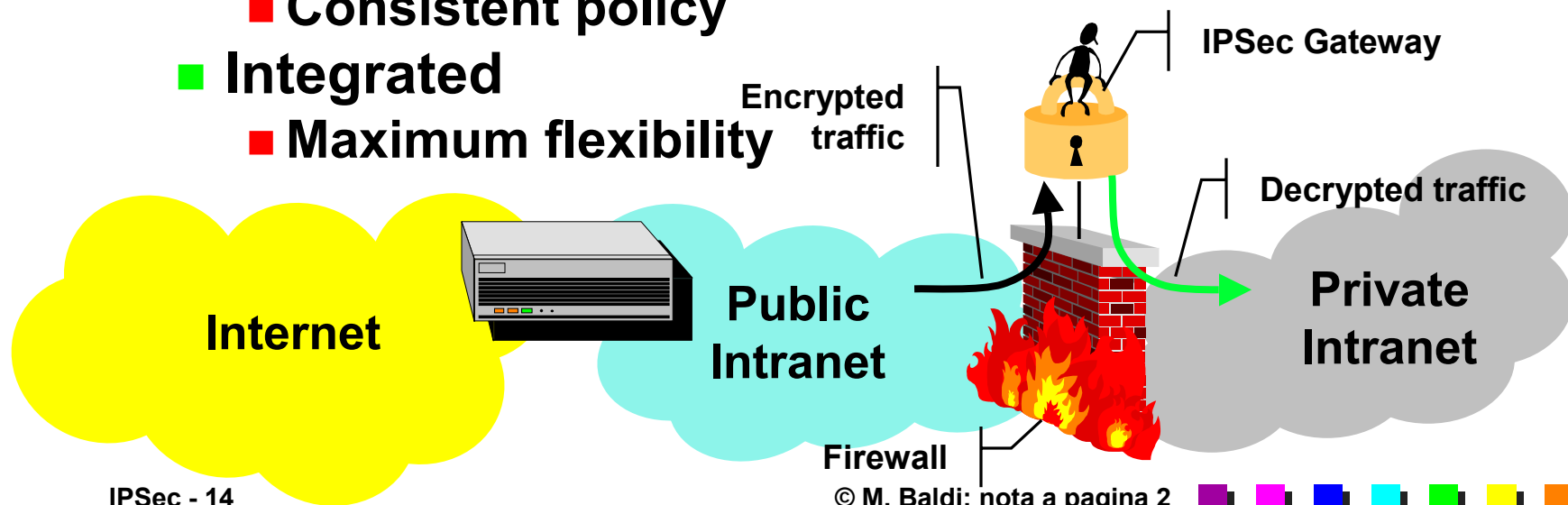


■ Autenticato

▨ Cifrato


IPSec Gateway and Firewall

- Inside
 - No inspection of encrypted traffic
 - IPSec gateway protected by firewall
- Parallel
 - Potential uncontrolled access
- Outside
 - IPSec gateway protected by access router
 - Consistent policy
- Integrated
 - Maximum flexibility





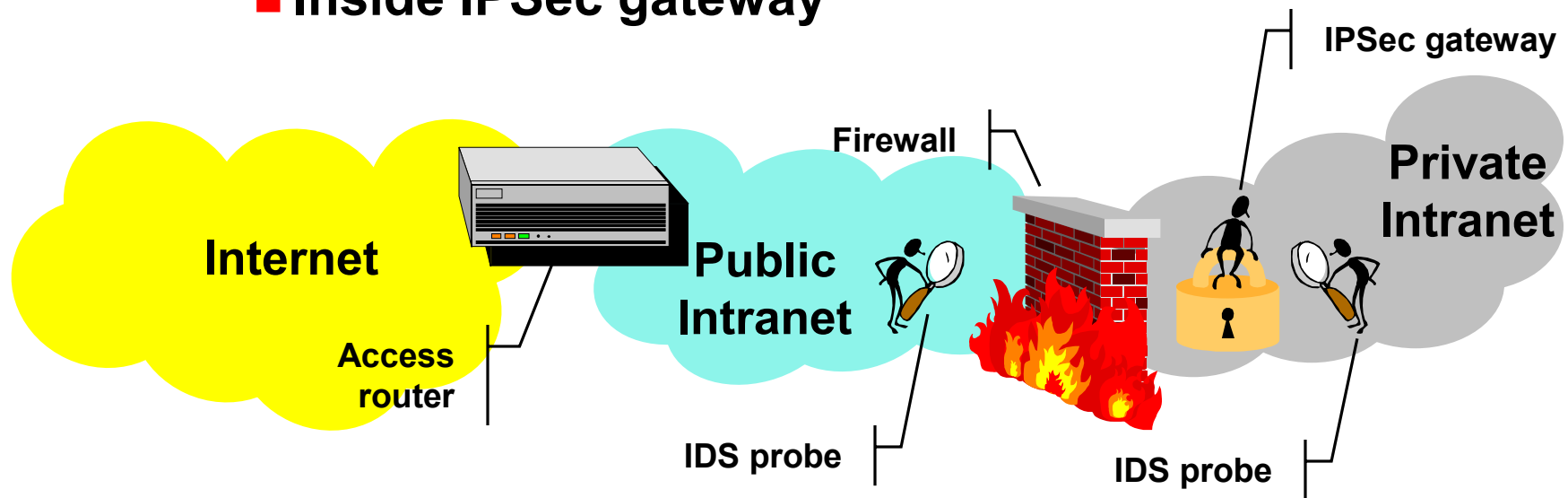
IPSec Gateway and NAT

- **Authentication Header (AH)**
 - IP addresses are part of AH checksum calculation → packets discarded
 - **Transport mode**
 - IP address of IPSec tunnel peer is not what expected → packets discarded
 - **No PAT (Protocol Address Translation)**
 - **Tunnel mode**
 - IP address within secure packet can be changed before entering the gateway
 - E.g., same addresses in two different VPN sites
 - Most often NAT is not needed on external packet
- 



IPSec Gateway and IDS

- IDS is usually outside the firewall
- No control on encrypted traffic
- Multiple IDS probes
 - Outside firewall
 - Inside IPSec gateway












Riferimenti bibliografici

- S. Kent and R. Atkinson, “Security Architecture for the Internet Protocol,” RFC 2401, November 1998.
- D. Harkins and D. Carrel, “The Internet Key Exchange (IKE),” RFC 2409, November 1998.
- S. Kent and R. Atkinson, “IP Encapsulating Security Payload (ESP),” RFC 2406, November 1998.
- S. Kent and R. Atkinson, “IP Authentication Header,” RFC 2402, November 1998.

