Securing Data with IPSec VPN

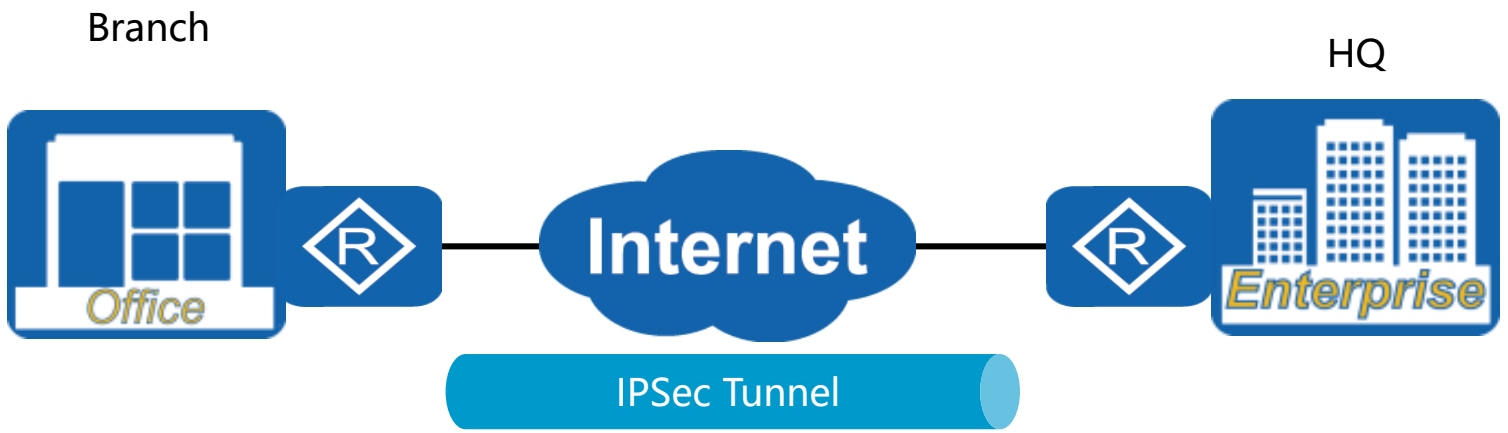
Foreword

- Early TCP/IP protocol development did very little for ensuring the security of communications between peering devices. As networks evolved so did the need for greater protection of the data transmitted. Solutions for data protection were developed, from which IPSec emerged as a security architecture for the implementation of confidentiality, integrity and data origin authentication, primarily through the support of underlying protocols. IPSec remains a key framework in the protection of data, which has seen an integration of IPSec components adopted into the next generation of TCP/IP standards.

Objectives

- Upon completion of this section, you will be able to:
  - Explain the basic principles of the IPSec security architecture.
  - Configure IPSec peering between two devices.

IPSec VPN Application



- Facilitates the establishment of private network communication over a public network infrastructure.

IPSec VPN Application

Confidentiality:

impedisce che il contenuto della comunicazione possa essere rilevato da altri. Anche il mittente, il destinatario, la lunghezza del messaggio e la frequenza di comunicazione sono protetti.

Integrity:

Connectionless – è un servizio che rileva la modifica di un datagramma IP senza tenere conto dell'ordine dei datagrammi nello stream; Viene anche definito anty-reply service

Connection Oriented

impone dei vincoli anche sulla sequenza dei datagrammi e può rilevare tentative di riordino dei frames.

Page 4

IPSec VPN Application

Availability:

protegge mittente e destinatario da attacchi che possono portare al degrado del servizio di comunicazione.

IPSec establishes **bidirectional security associations between IPSec peers** to form a secure IPSec tunnel**, imports data flows to be protected** to the tunnel, and then **uses security protocols to encrypt and authenticate the data** passing through the tunnel to securely transmit the data over the Internet.

IPSec SAs can be established manually or through IKEv1 or IKEv2 auto-negotiation.

Page 5

IPSec VPN Architecture

AH – Authentication Header

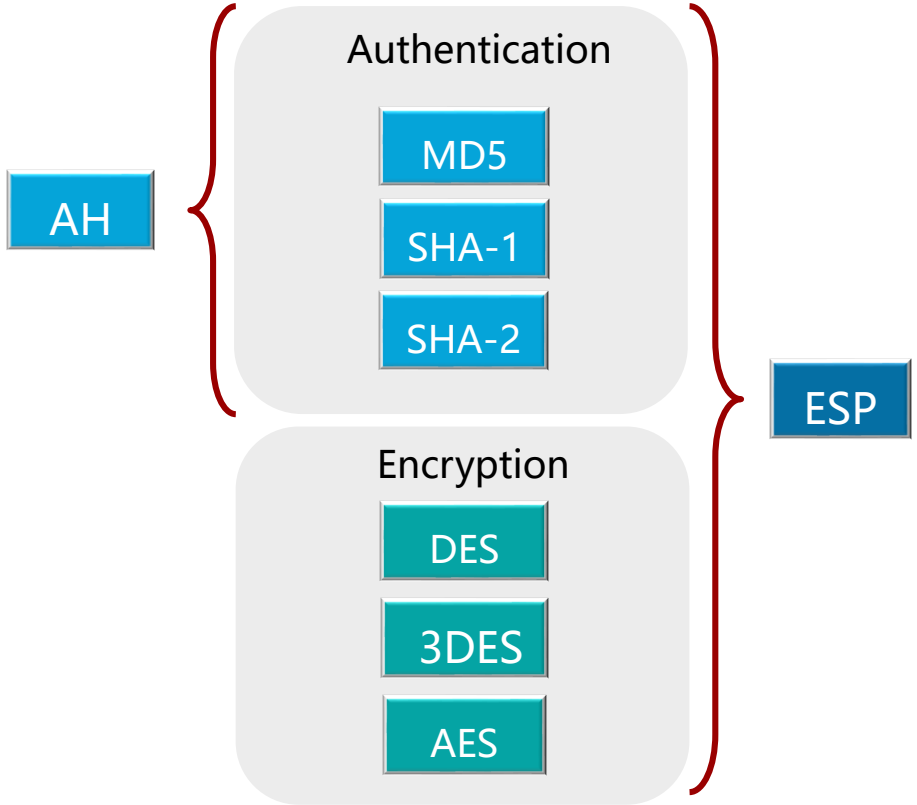
- Connectionless integrity
- data origin authentication
- anti-replay
- Protocol type: 51 – RFC 2442

ESP – Encapsulating Security Payload

- Confidentiality
- Traffic flow confidentiality
- Optional authentication
- Protocol type: 50 – RFC 2406

Page 6

IPSec VPN Architecture



- Confidentiality and integrity of services are supported through authentication and encryption based protocols.

Security Association

SA

E’ la policy che viene condivisa tra due peer o due hosts e che definisce quali saranno i servizi IPSec utilizzati per proteggere il traffico.

Caratteristiche della SA:

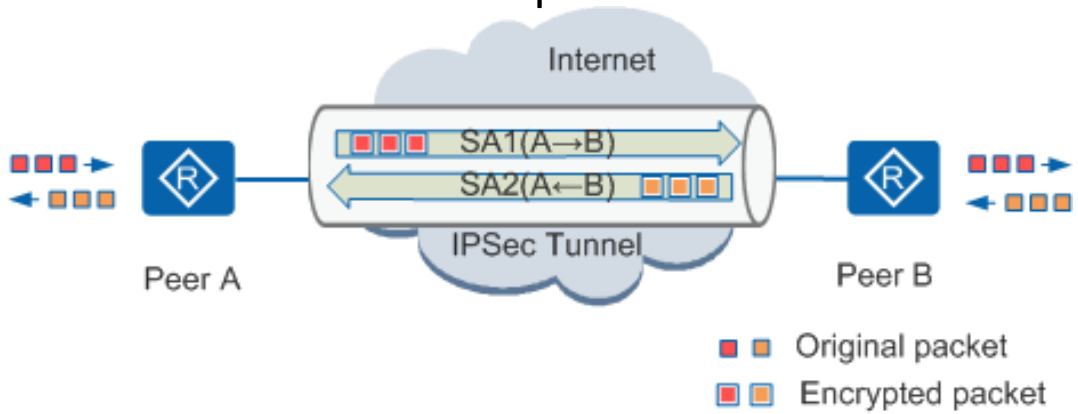
- **Monodirezionale**: serve una SA per definire i parametri della connessione tra R1 ed R2 ed una diversa per la connessione tra R2 ed R1.
- **Monoprotocollo**: una SA distinta per AH ed ESP;
- **Tempo limitata**: le SA scadono!

Page 8

Security Association

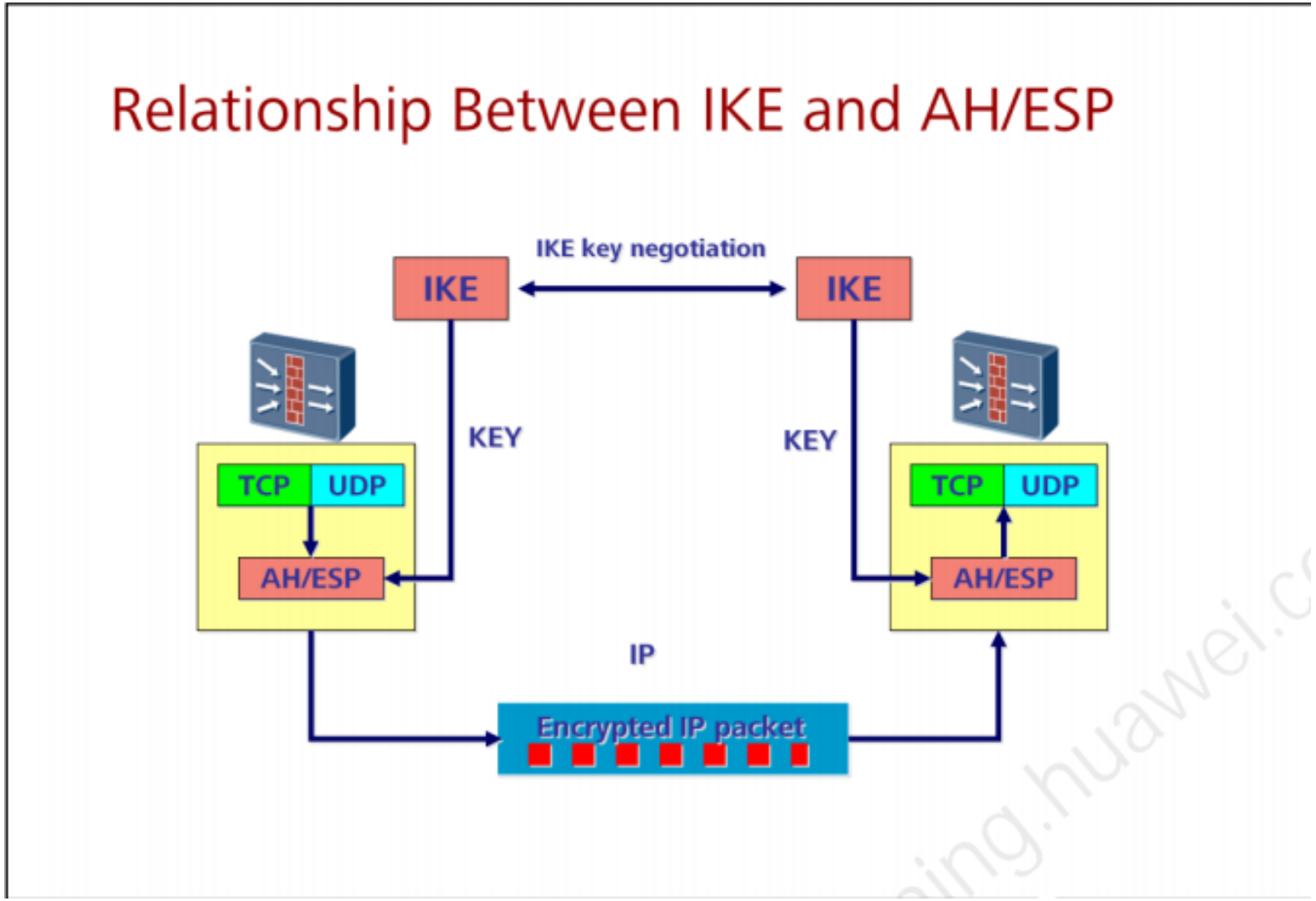
SA – può essere definita:

- **Manualmente**
- **Attraverso IKE** (internet Key Exchange) con il supporto ai protocolli:
  - ISAKMP
  - OAKLEY
  - Scheme
- Proteggere lo scambio delle SA e autenticare il peer.

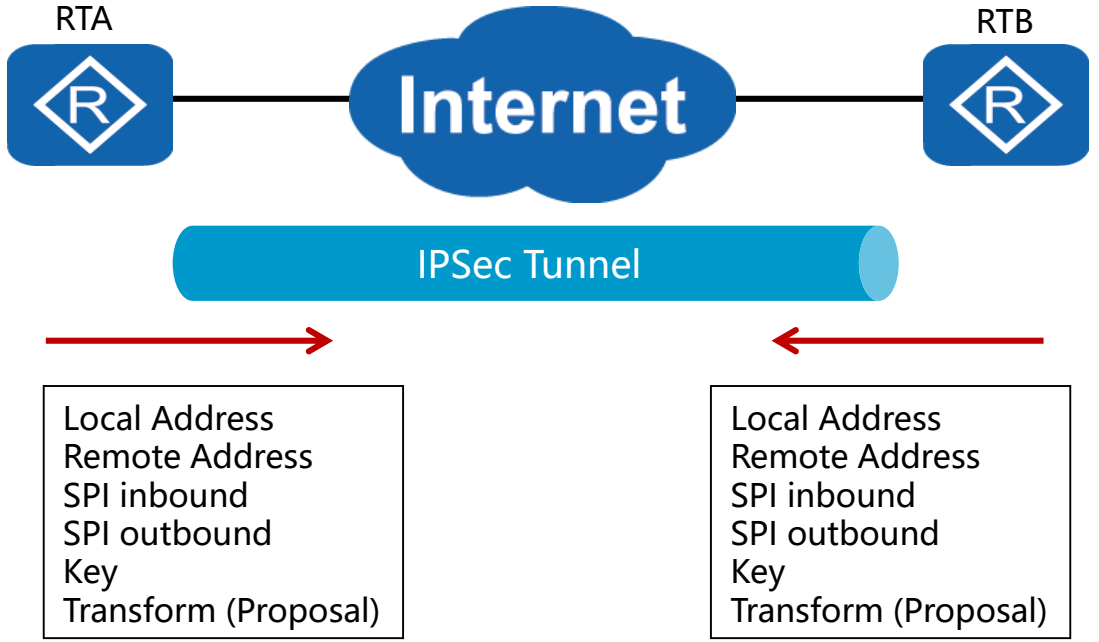


Page 9

Security Association



Security Association



- Specifies parameters for connection establishment.
- A Security Association defines parameters in only one direction.

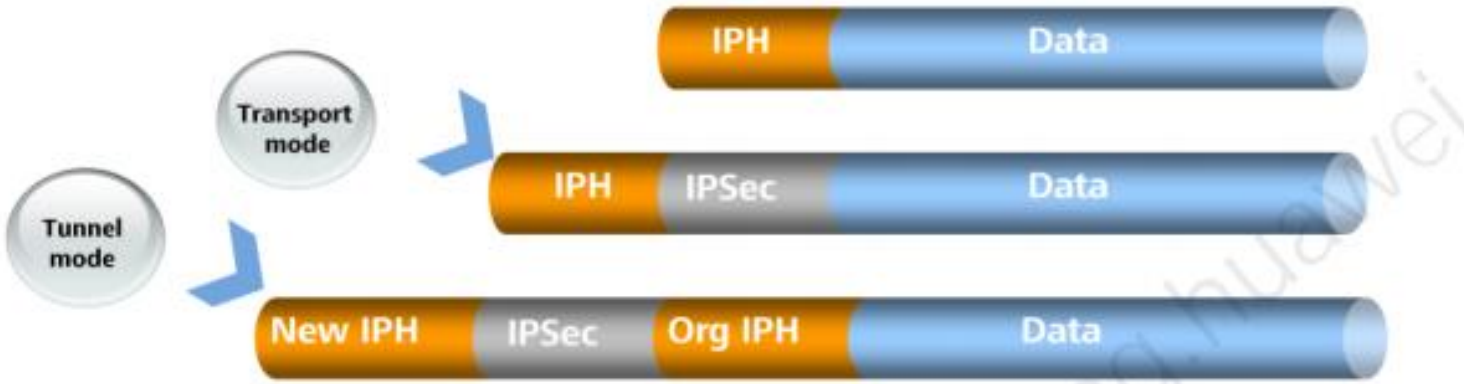
IPSec Encapsulation Modes

Transport mode

- IPSec headers are inserted behind the IP header and before all transport layer protocols or all other IPSec protocols.

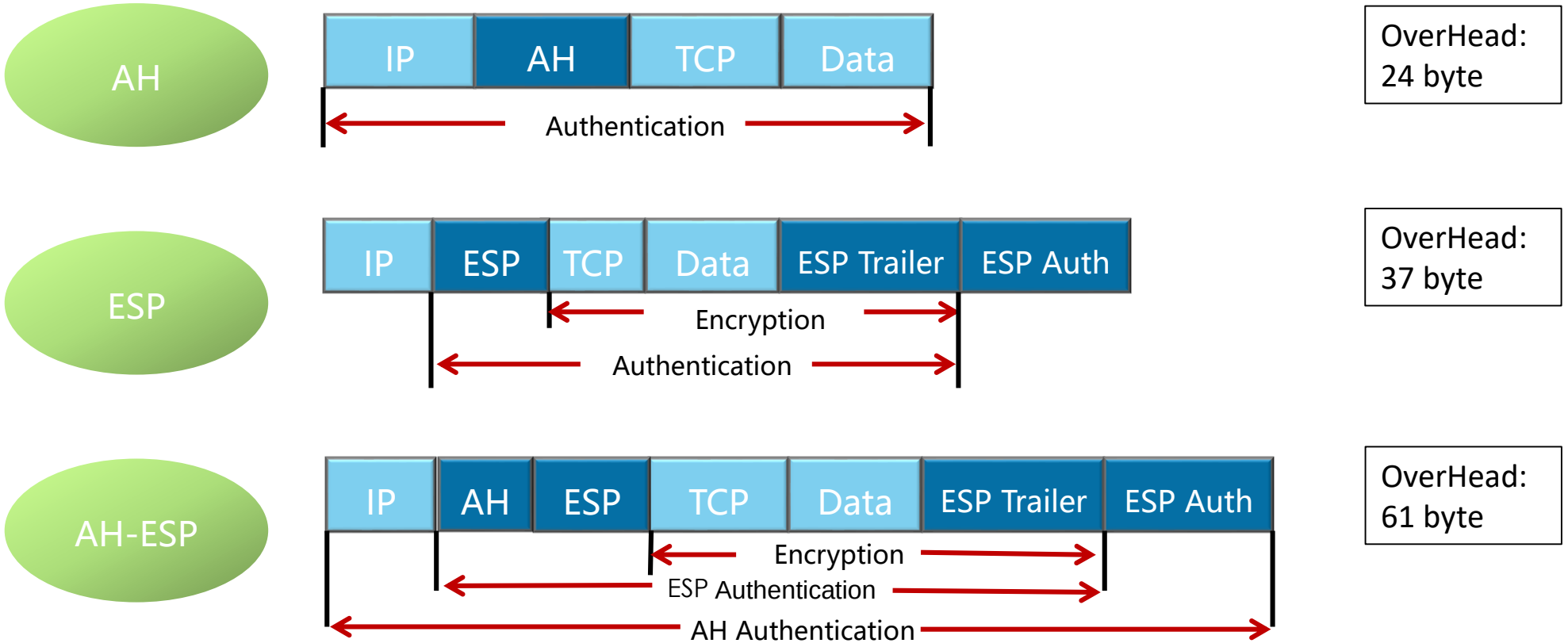
Tunnel mode

- IPSec headers are inserted before the original IP header. The new packet header is placed before AH or ESP.



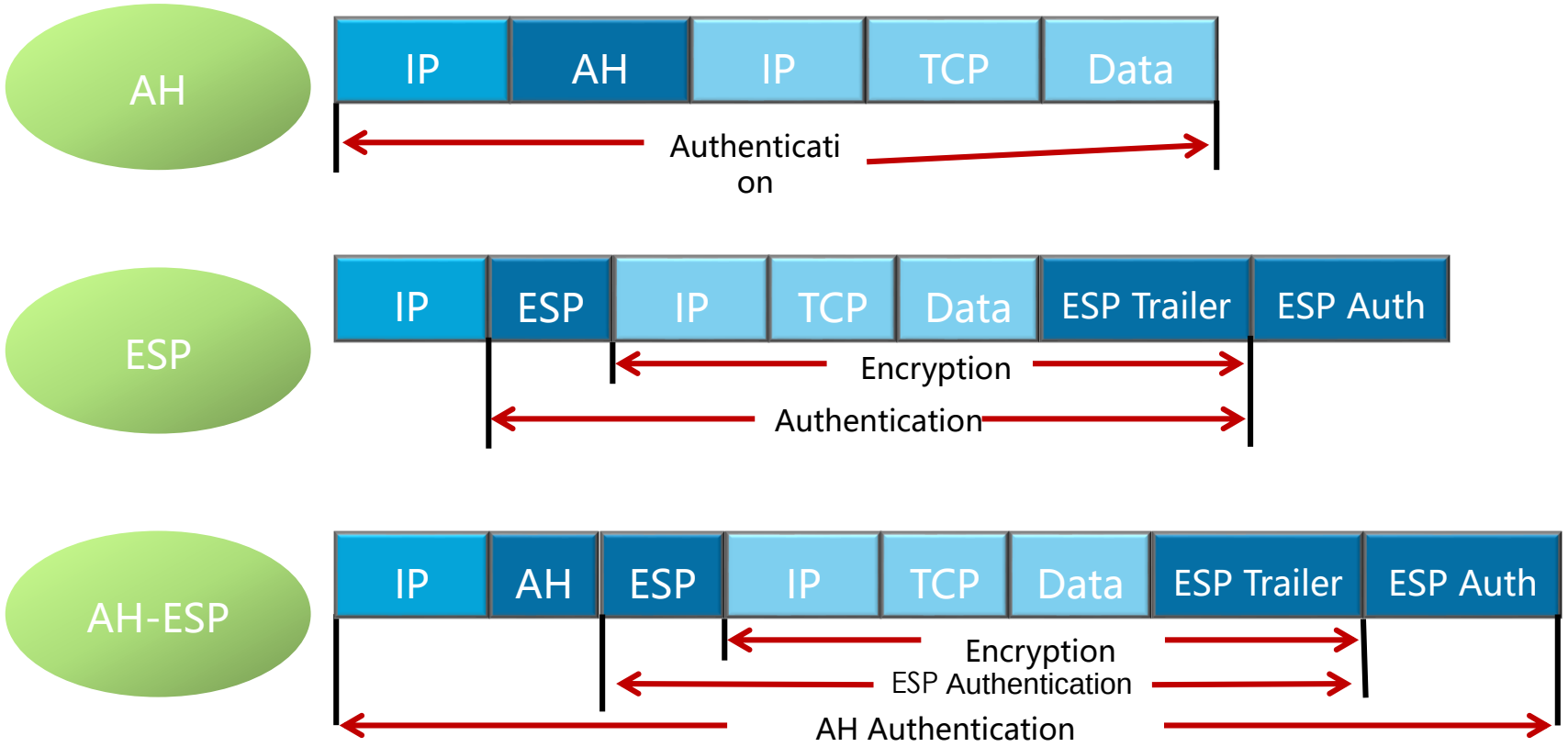
Page 12

IPSec Transport Mode



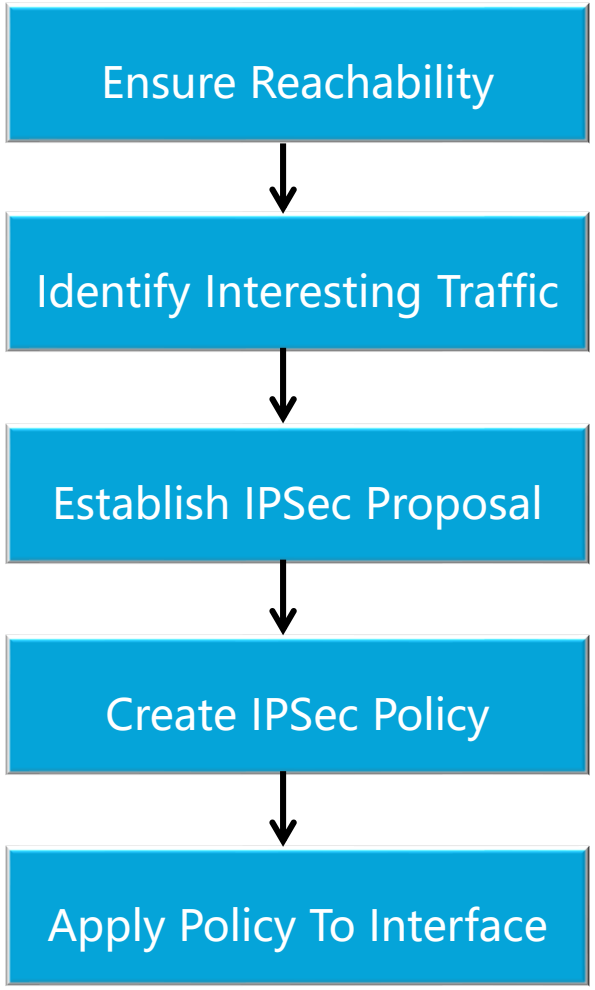
- Encapsulation modes are defined in Security Associations.
- Transport mode secures only the payload of the packet.

IPSec Tunnel Mode



- Tunnel mode encapsulates packets in a second IP header.
- Security is extended to the inner IP header and packet payload.

IPSec VPN Establishment



Configurazione – altro punto di vista!

Step necessari:

- Individuare il traffico da proteggere con una o più ACL;
- IKE fase 1
  - Autenticazione dei peer
  - IKE SA
  - Stabilire un canale per la negoziazione delle SA
- IKE fase 2
  - Negoziazione delle IPSec SA
  - Impostazione delle SA nei peer.

Page 16

Configurazione – altro punto di vista!

acl <acl_number>

rule 5 permit ip source <ips> <wcs> destination <ipd> <wcd>

ipsec proposal <proposal_name>

encapsulation-mode <transport | tunnel>

transform <ah | esp | ah-esp >

esp authentication-algorithm < ... >

esp encryption-algorithm < ... >

ah authentication-algorithm < ... >

Page 17

Configurazione – altro punto di vista!

ike peer <peer_name> <v1 | v2 >

pre-shared-key <cipher | simple > <peer_key>

remote-address <peer_ip>

ipsec policy <policy_name> <sequence_number> <isakmp | manual >

proposal <proposal_name>

security acl <acl_number>

se hai scelto **isakmp**: ike-peer <peer_name>

se hai scelto **manual** ->

Page 18

Configurazione – altro punto di vista!

tunnel remote <peer_ip_remote>

tunnel local <local_ip_address>

sa spi outbount esp <id1>

sa spi inbound esp <id2>

sa string-key outbound esp simple <pass1>

sa string-key inbound esp simple <pass2>

sa spi outbount ah <id1>

sa spi inbound ah <id2>

sa string-key outbound ah simple <pass1>

sa string-key inbound ah simple <pass2>

Page 19

IpSec policy template

An IPSec policy template can be used to configure multiple IPSec policies, reducing the workload of establishing multiple IPSec tunnels.

ipsec policy-template <template_name> <sequence_number>

security acl <number>

proposal <name>

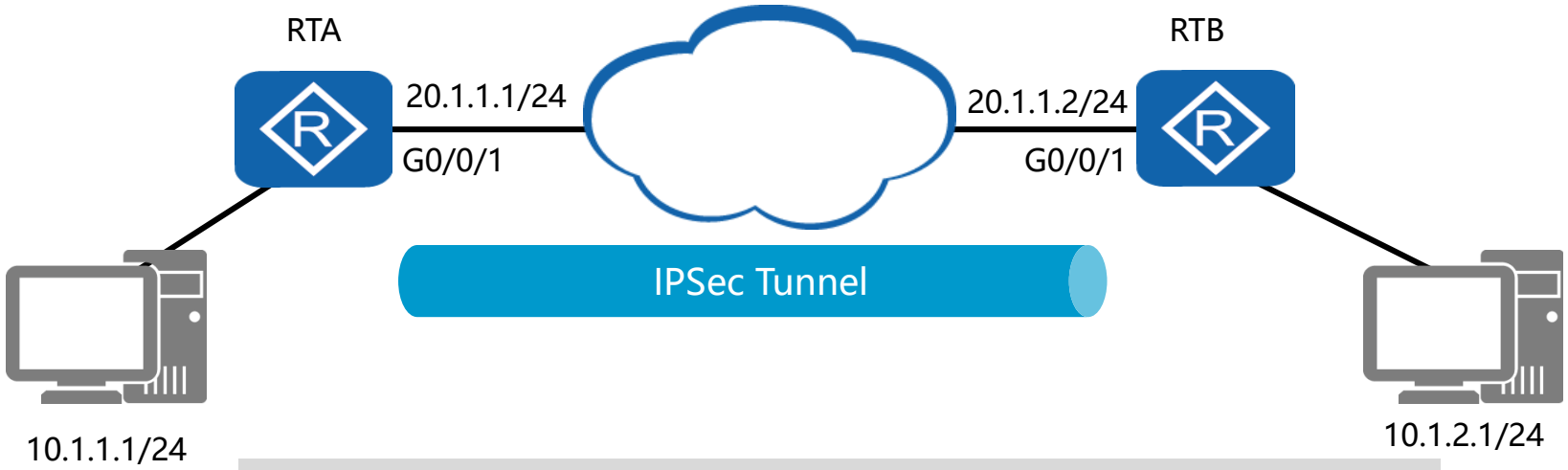
ike-peer <peer_name>

Utilizzare il template per una policy (in system-view):

ipsec policy <policy_name> <sequence> isakmp template <template_name>

Page 20

IPSec VPN Configuration




```
[RTA]ip route-static 10.1.2.0 24 20.1.1.2
[RTA]acl number 3001
[RTA-acl-adv-3001]rule 5 permit ip source 10.1.1.0
 0.0.0.255 destination 10.1.2.0 0.0.0.255
[RTA]ipsec proposal tran1
[RTA-ipsec-proposal-tran1]esp authentication-algorithm
 sha1
```

IPSec VPN Proposal Verification

```
[RTA]display ipsec proposal
 Number of proposals : 1
 IPSec proposal name : tran1
 Encapsulation mode  : Tunnel
 Transform           : esp-new
 ESP protocol        : Authentication SHA1-HMAC-96
                       Encryption     DES
```

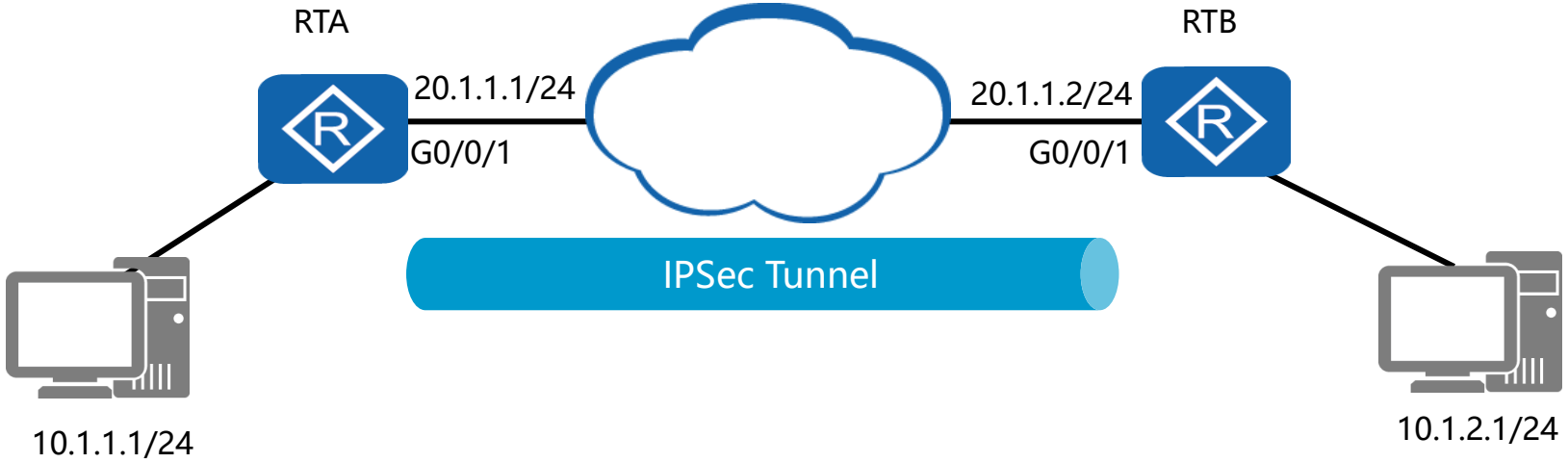
- Displays the parameters of an IPSec proposal.
- Proposal parameters must match for both peering interfaces.

IPSec Policy Creation

```
[RTA]ipsec policy P1 10 manual
[RTA-ipsec-policy-manual-P1-10]security acl 3001
[RTA-ipsec-policy-manual-P1-10]proposal tran1
[RTA-ipsec-policy-manual-P1-10]tunnel remote 20.1.1.2
[RTA-ipsec-policy-manual-P1-10]tunnel local 20.1.1.1
[RTA-ipsec-policy-manual-P1-10]sa spi outbound esp 54321
[RTA-ipsec-policy-manual-P1-10]sa spi inbound esp 12345
[RTA-ipsec-policy-manual-P1-10]sa string-key outbound esp simple huawei
[RTA-ipsec-policy-manual-P1-10]sa string-key inbound esp simple huawei
```

- IPSec policy defines parameters for establishing an IPSec SA.
- An IPSec policy binds the proposal parameters and traffic filters.

Applying Policies to Interfaces




```
[RTA]interface GigabitEthernet 0/0/1
[RTA-GigabitEthernet0/0/1]ipsec policy P1
[RTA-GigabitEthernet0/0/1]quit
```

- The IPSec policy is bound to the physical interface via which the IPSec peer is reachable.

IPSec Policy Verification

```
[RTA]display ipsec policy
==========================================
IPSec policy group: "P1"
Using interface: GigabitEthernet0/0/1
==========================================
    Sequence number: 10
    Security data flow: 3001
    Tunnel local  address: 20.1.1.1
    Tunnel remote address: 20.1.1.2
    Qos pre-classify: Disable
    Proposal name:tran1
...
```

- Policy must associate with the policy of the peering interface.

IPSec Policy Verification

```
...
Inbound ESP setting:
      ESP SPI: 12345 (0x3039)
      ESP string-key: huawei
      ESP encryption hex key:
      ESP authentication hex key:
   Outbound ESP setting:
      ESP SPI: 54321 (0xd431)
      ESP string-key: huawei
      ESP encryption hex key:
      ESP authentication hex key:
...
```

- Policy Key strings must match for communication to establish.

Summary

- What is meant by a Security Association (SA)?
- What are the three possible actions that may be applied to IPSec filtered traffic?


Thank You
www.huawei.com