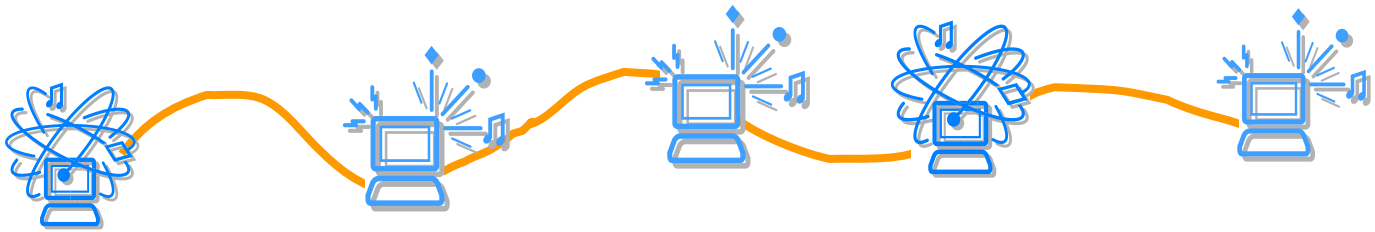
Segurança em Redes
VPN – IPsec



Redes de Comunicação
Departamento de Engenharia da Electrónica e Telecomunicações e de Computadores
Instituto Superior de Engenharia de Lisboa

IPsec

Características básicas

- IPsec fornece segurança na camada de rede (Internet).
  - Todos os pacotes IP estão cobertos
  - Não é necessária a remodelação das aplicações
  - Transparente para os utilizadores.

- Implementação obrigatória para o IPv6, opcional para a geração actual do IP (IPv4).

- Definido no IETF RFCs 4301– 4308 (são muitos ☹). Mas há ainda mais!

RFC

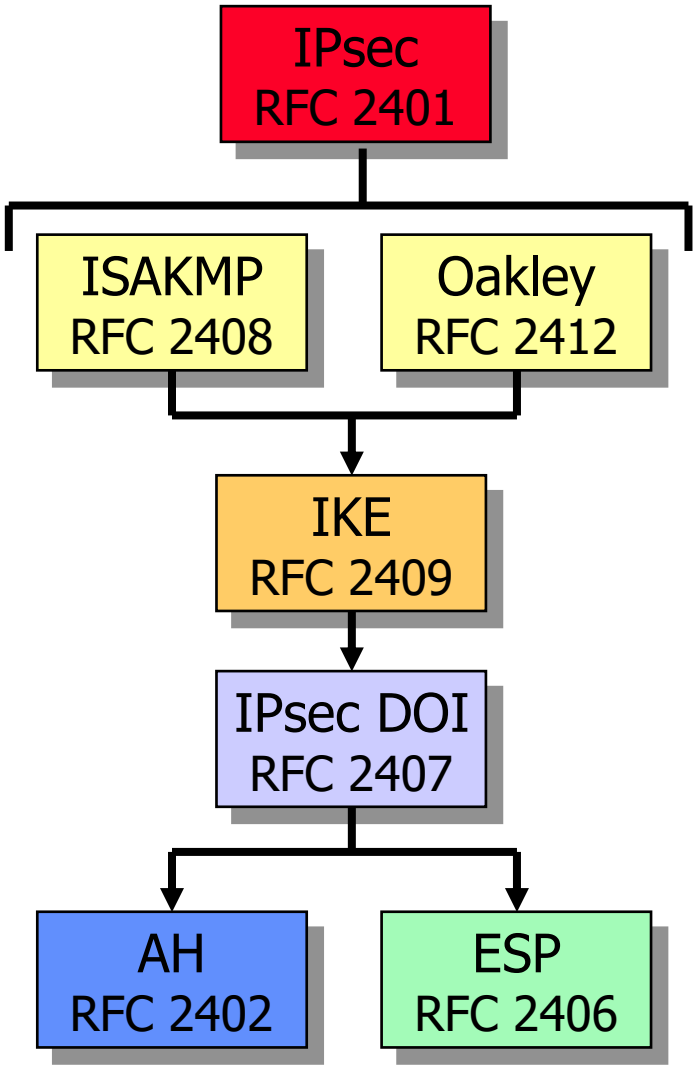
- RFCs 2401 - 2412 (a **maioria obsoleta** pelos RFCs 40XX)

- RFC 4301 (*Security Architecture for the Internet Protocol*)
- RFC 4302 (IP Authentication Header)
- RFC 4303 (IP Encapsulating Security Payload (ESP))
- RFC 4304 (Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP))
- RFC 4305 (Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH))
- RFC 4306 (Internet Key Exchange (IKEv2) Protocol)

RFC

- RFC 4307 (Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2))
- RFC 4308 (Cryptographic Suites for IPsec)
- RFC 4309 (Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP))
- RFC 4312 (The Camellia Cipher Algorithm and Its Use With IPsec)
- RFC 3740 (*The Multicast Group Security Architecture*)

RFC mais importantes (obsoleto)

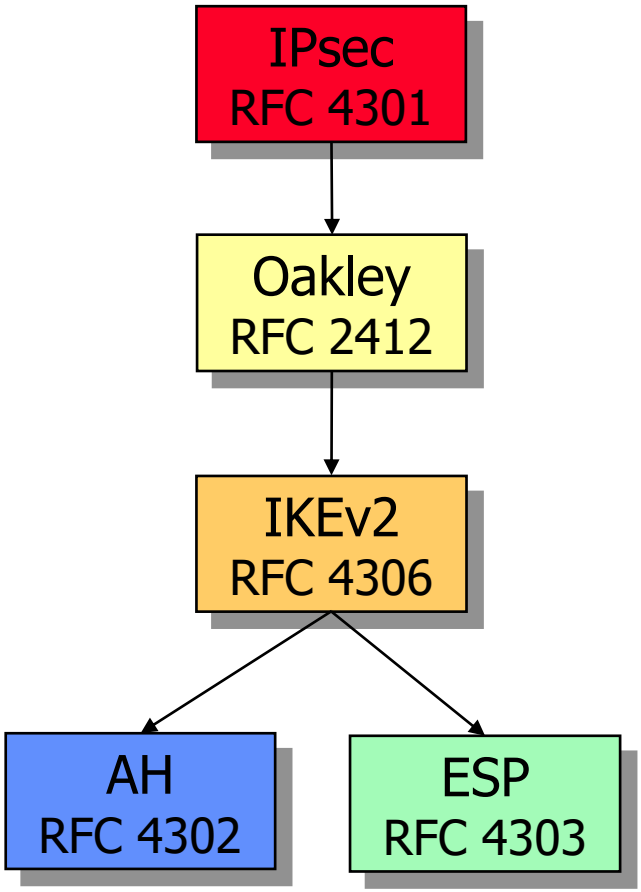


O IKEv2 não é compativel com o IKEv1

ISAKMP	Internet Security Association and Key Management Protocol
IKE	Internet Key Exchange
DOI	Domain of Interpretation
AH	Authentication Header
ESP	Encapsulating Security Payload

RFC mais importantes

O IKEv2 não é compatível com o IKEv1



ISAKMP	Internet Security Association and Key Management Protocol
IKE	Internet Key Exchange
DOI	Domain of Interpretation
AH	Authentication Header
ESP	Encapsulating Security Payload

Conjunto de serviços de segurança oferecido

- Confidencialidade (cifra) dos conteúdos das mensagens
- Confidencialidade limitada do fluxo de tráfego
  - –Não se consegue saber o endereço de quem está a enviar dados (modo túnel).
- Autenticação da origem dos dados
- Integridade na ligação *connectionless*
- Integridade parcial da sequência
  - *Connectioless:* Integridade de cada pacote IP
  - Integridade parcial da sequência: Evita ataques por repetição
- Controlo de acessos
- Protecção limitada contra ataques DoS
- Compressão IP

Componentes fundamentais da arquitectura de segurança

- Protocolos de segurança:
  - ***Authentication Header* (AH)** e ***Encapsulating Security Payload* (ESP)**

- Associações de segurança (SA) – o que são, como funcionam, como são geridas, processamento associado?

- Gestão de chaves
  - Manual
  - Automática (*Internet Key Exchange* (IKE))

- Algoritmos para autenticação e cifra

IPsec

IPsec = AH + ESP + IPcomp + IKE

Protecção do tráfego IP. O AH fornece integridade e autenticação da origem. O ESP fornece também confidencialidade.

Compressão

Inicia as chaves e os algoritmos para o AH e o ESP

O AH e o ESP suportam-se nas associações de segurança (SA) criadas

Ideia: As partes devem partilhar um conjunto de chaves secretas e acordar sobre os endereços IP e os algoritmos de segurança a utilizar .

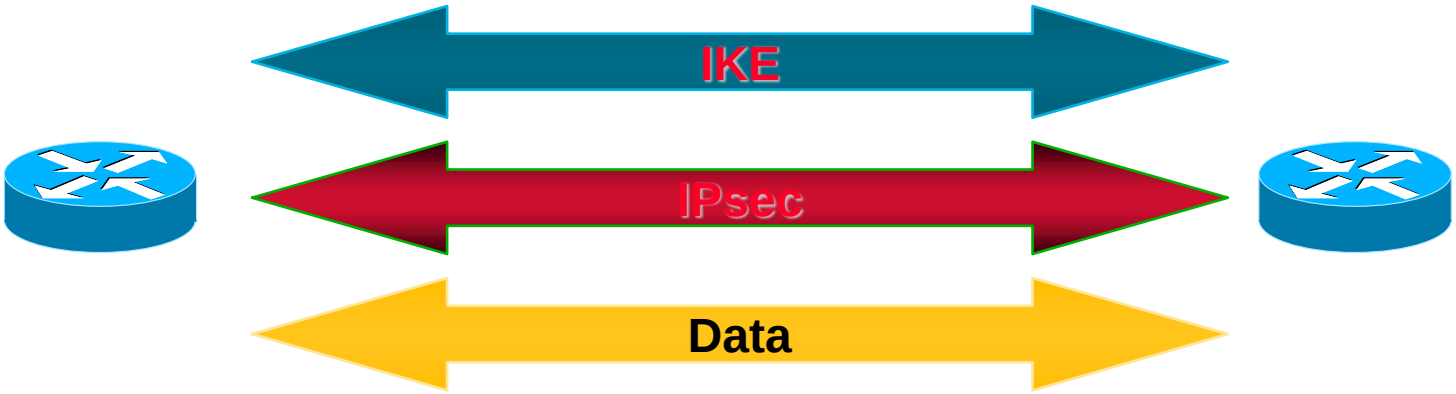
IKE – *Internet Key Exchange*

Objectivo: Estabelecer associações de segurança para o AH e o ESP

Se o IKE for "quebrado", o AH e o ESP deixam de proteger.

	Modo transporte SA	Mode túnel SA
AH	Autentica a carga e partes seleccionadas do cabeçalho IP e extensões ao cabeçalho no IPv6.	Autentica todo o pacote IP interior mais porções seleccionadas do cabeçalho IP exterior.
ESP	Cifra a carga IP e qualquer extensão ao cabeçalho no IPv6.	Cifra todo o pacote IP interior.
ESP com autenticação	Cifra a carga IP e qualquer extensão ao cabeçalho no IPv6. Autentica a carga IP mas não o cabeçalho.	Cifra o pacote IP interior. Autentica o pacote IP interior.

Iniciar novas ligações



- Estabelecer **SA IKE**
- Estabelecer **SA IPsec**
  - Múltiplos SA IPsec para cada IKE SA
- Envio de dados protegidos

Modularidade

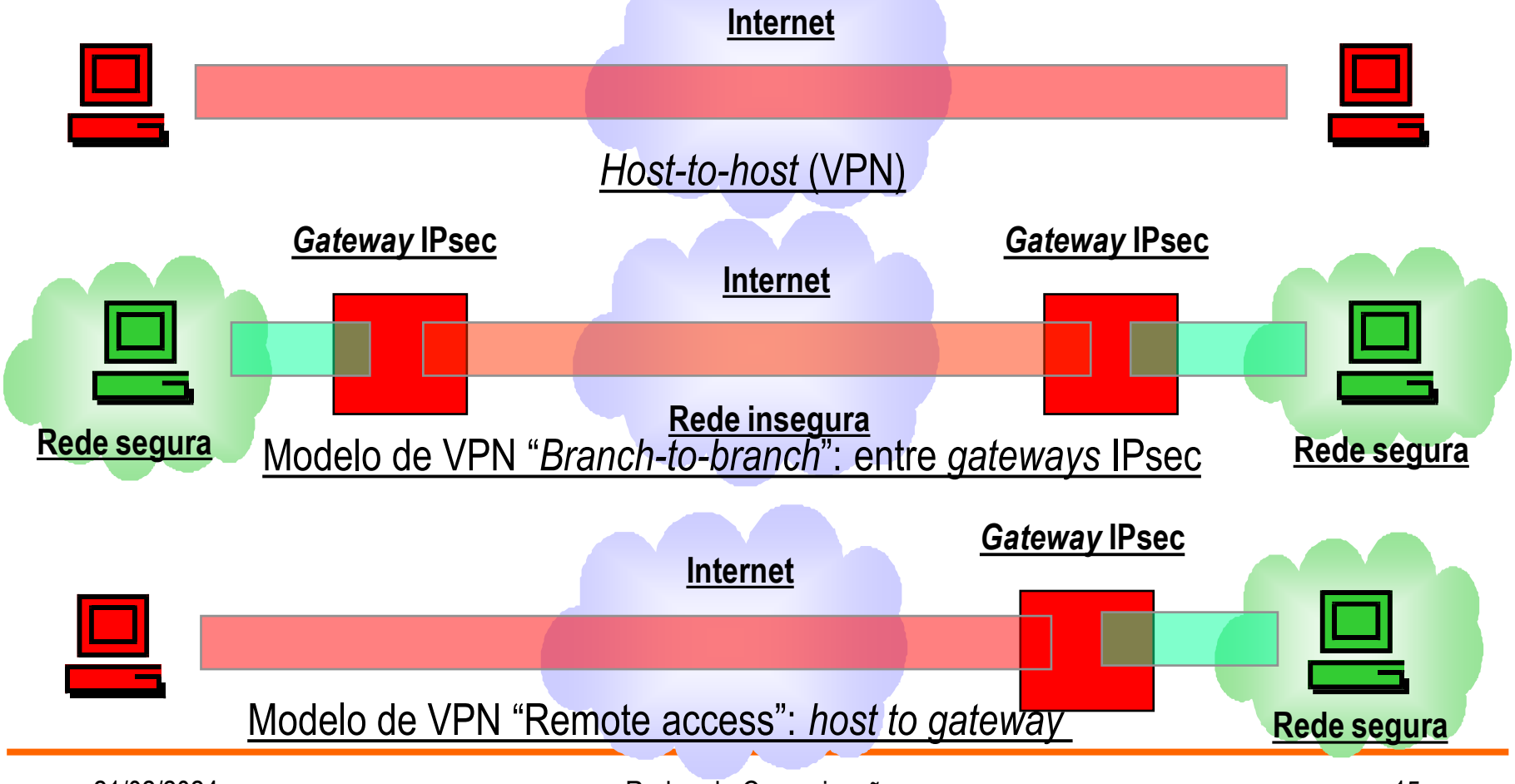
- **Mecanismos do IPsec independentes dos algoritmos de segurança**.

- **Permite a selecção de diferentes conjuntos de algoritmos** sem afectar outras partes da implementação.

- Comunidades diferentes de utilizadores podem utilizar diferentes conjuntos de algoritmos.

Modelos de VPN utilizando IPsec

Opera num *host* ou num *gateway* de segurança (*router*, concentrador de VPN, *firewall*, …) fornecendo segurança ao tráfego IP.



Protocolos de suporte à segurança do tráfego

- IPsec utiliza dois protocolos:
  - **AH (*Authentication Header);* ESP (*Encapsulating Security Payload*)**
- **Protocolo AH** fornece:
  - Integridade *connectionless*,
  - Autenticação da origem dos dados
  - Serviço opcional de protecção anti-repetição.
- **Protocolo ESP** fornece :
  - Confidencialidade
  - Confidencialidade limitada do fluxo de tráfego
  - Integridade *connectionless*
  - Autenticação da origem dos dados
  - Serviço opcional de protecção anti-repetição.
- Ambos dão suporte para o **controlo de acessos** baseado na distribuição de chaves criptográficas

Protocolos de suporte à segurança do tráfego

- Os protocolos AH e ESP podem ser aplicados em conjunto ou separadamente.
- Cada um dos protocolos, AH e ESP, suporta **dois modos de utilização**:
  - **Modo "transporte"**: Para os *hosts IPsec-aware* como extremos.
  - **Modo "túnel"**: Para *hosts IPsec-unaware*, estabelecido por *gateways* intermédios.
  - Um *host* deve suportar o modo de transporte e o modo túnel.
  - Um *gateway* de segurança apenas necessita suportar modo túnel. Se suportar o modo transporte este deve ser usado apenas quando o *gateway* de segurança estiver a actuar como *host* (e.g. na gestão)
- O IPSec permite ao utilizador ou administrador **controlar a granularidade do serviço de segurança** oferecido, por exemplo:
  - Criar um túnel cifrado para transportar todo o tráfego entre dois *gateways* de segurança
  - Criar um túnel cifrado diferente para cada ligação TCP de cada par de *hosts* que comunicam através desse *gateway*

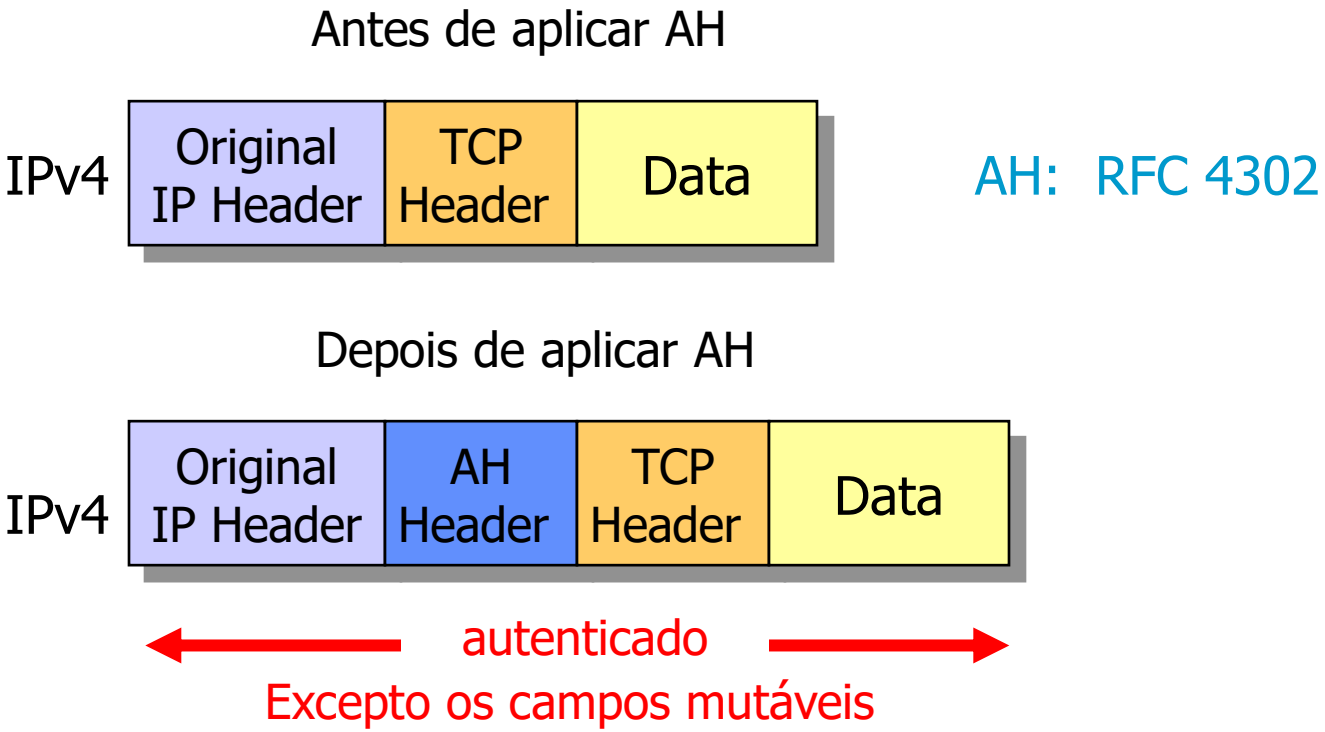
Encapsulamento AH e ESP

- **Modo transporte**
  - Quando são utilizados ambos os modos de segurança o *header* AH aparece primeiro no datagrama IPsec e só depois aparece o *header* ESP. Em termos de aplicação o ESP é aplicado primeiro e só depois é aplicado o AH.

- **Modo túnel**
  - A encapsulamento pode implicar o aparecimento em qualquer ordem dos *headers* AH e ESP dado o encapsulamento poder ir sendo realizado em vários locais ao longo do caminho.

Modo transporte usando AH

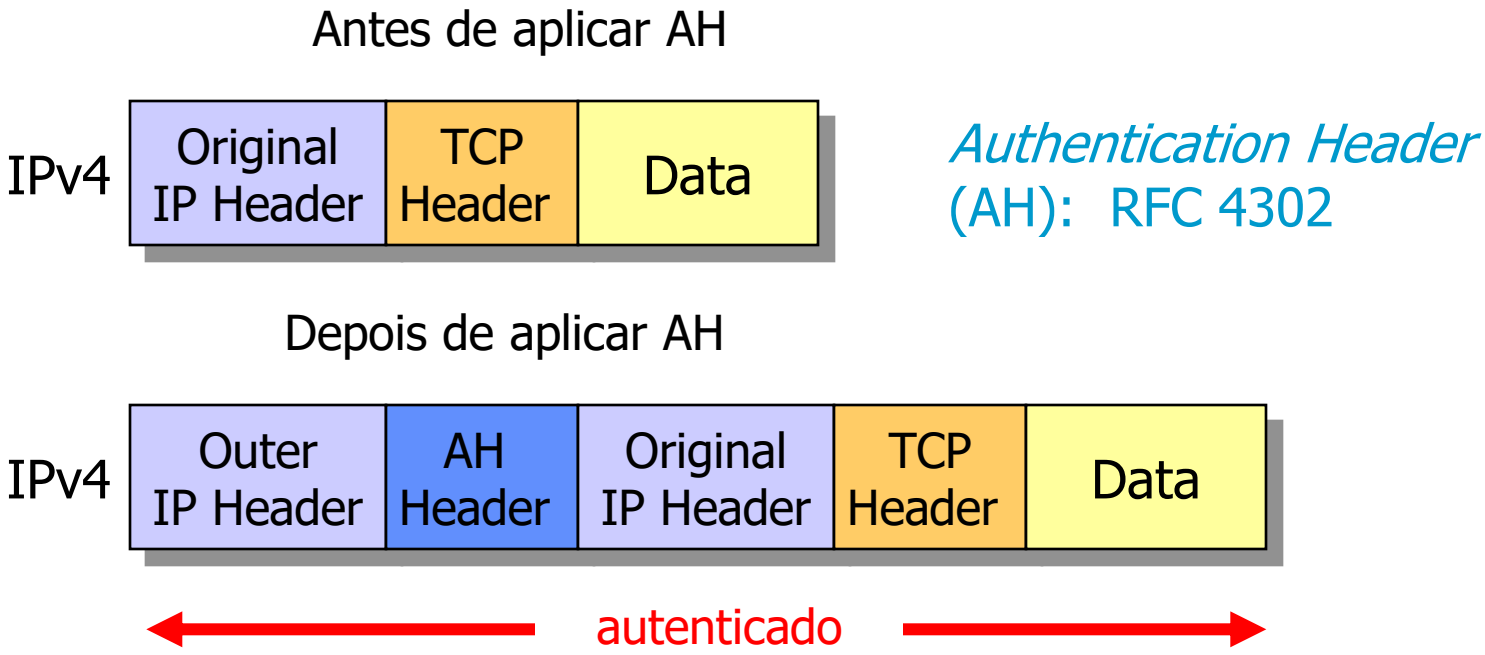
Authentication Header (AH)



- Número de protocolo IP para o AH: 51
- Campos mutáveis no *header* IP exterior não são autenticados: *Type of Service* (TOS), *Fragment Offset*, *Flags*, *Time to Live* (TTL), *Checksum* do cabeçalho IP

Modo túnel usando AH

Authentication Header (AH)

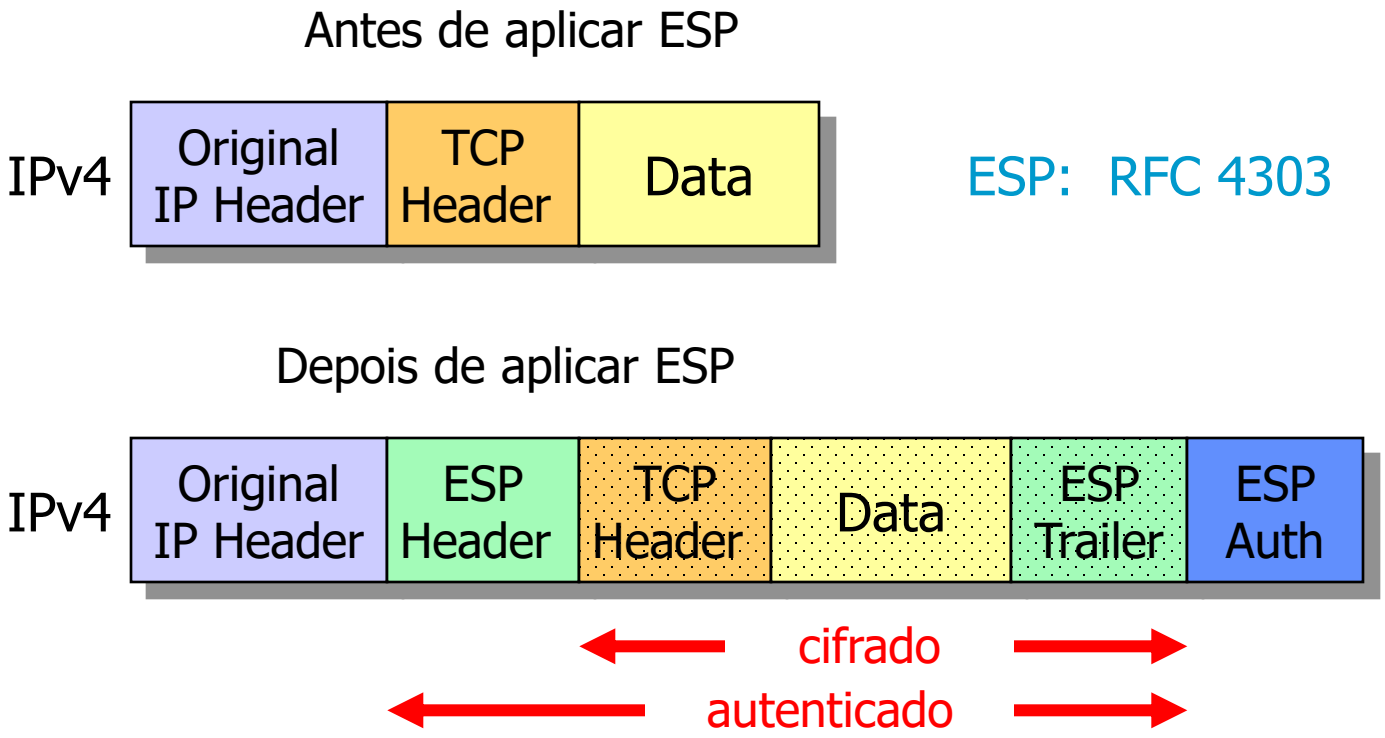


Authentication Header (AH): RFC 4302

- Número de protocolo IP para o AH: 51
- Campos mutáveis no *header* IP exterior não são autenticados: *Type of Service* (TOS), *Fragment Offset*, *Flags*, *Time to Live* (TTL), *Checksum* do cabeçalho IP

Modo transporte usando ESP

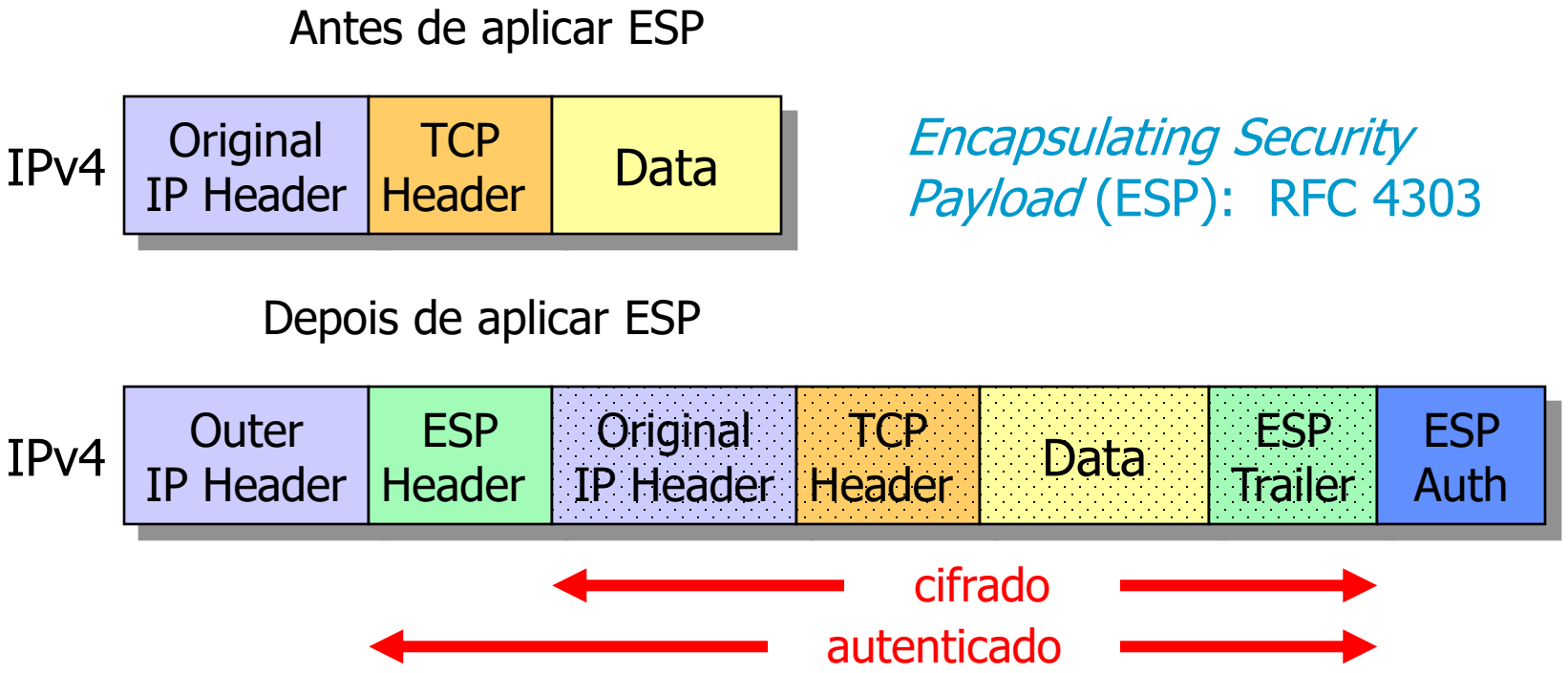
IP *Encapsulating Security Payload* (ESP)



- Protocolo IP para o ESP, número: 50
- A autenticação ESP é opcional
- Com a autenticação ESP o cabeçalho IP não é protegido.

Modo túnel usando ESP

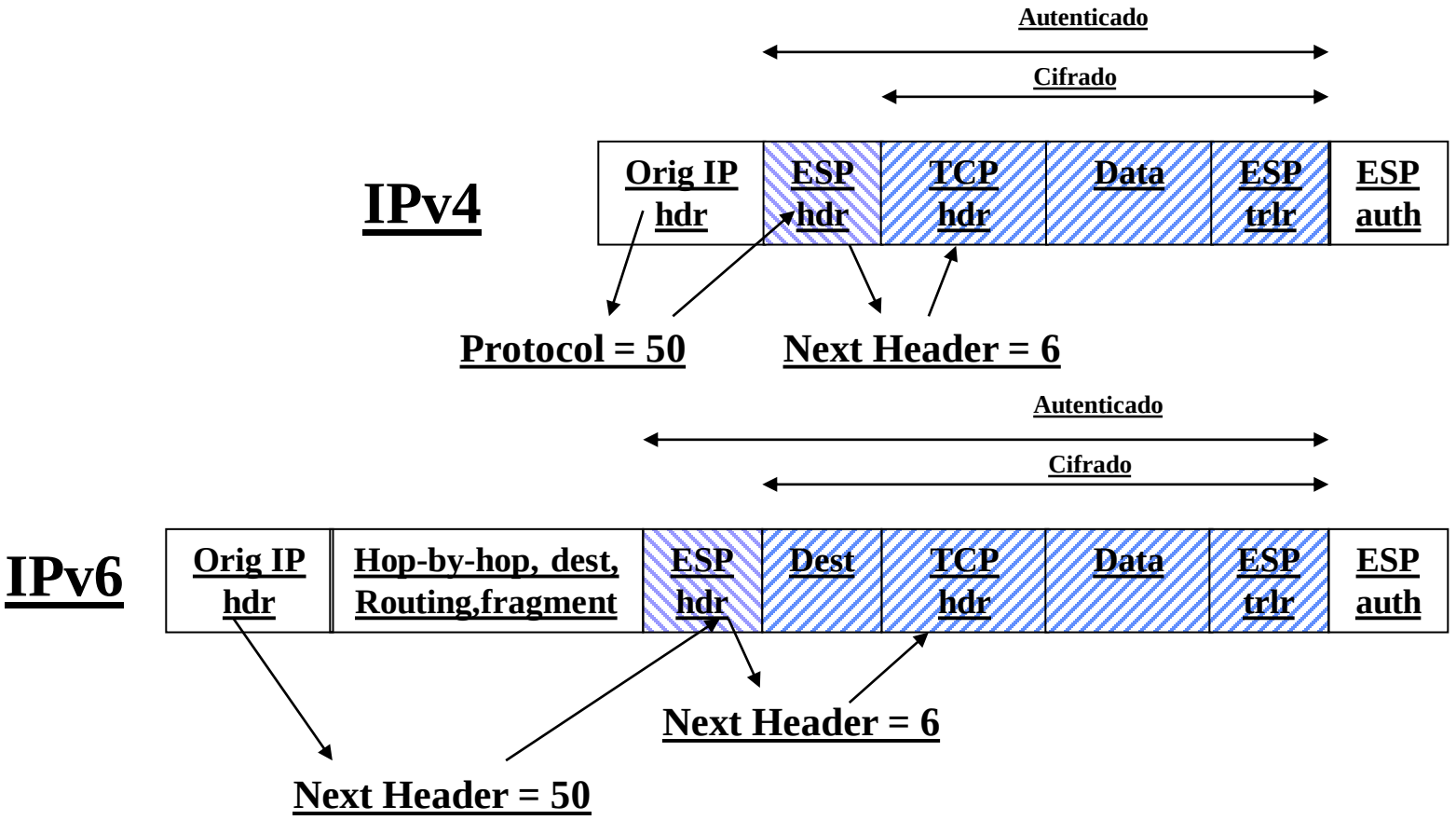
IP *Encapsulating Security Payload* (ESP)



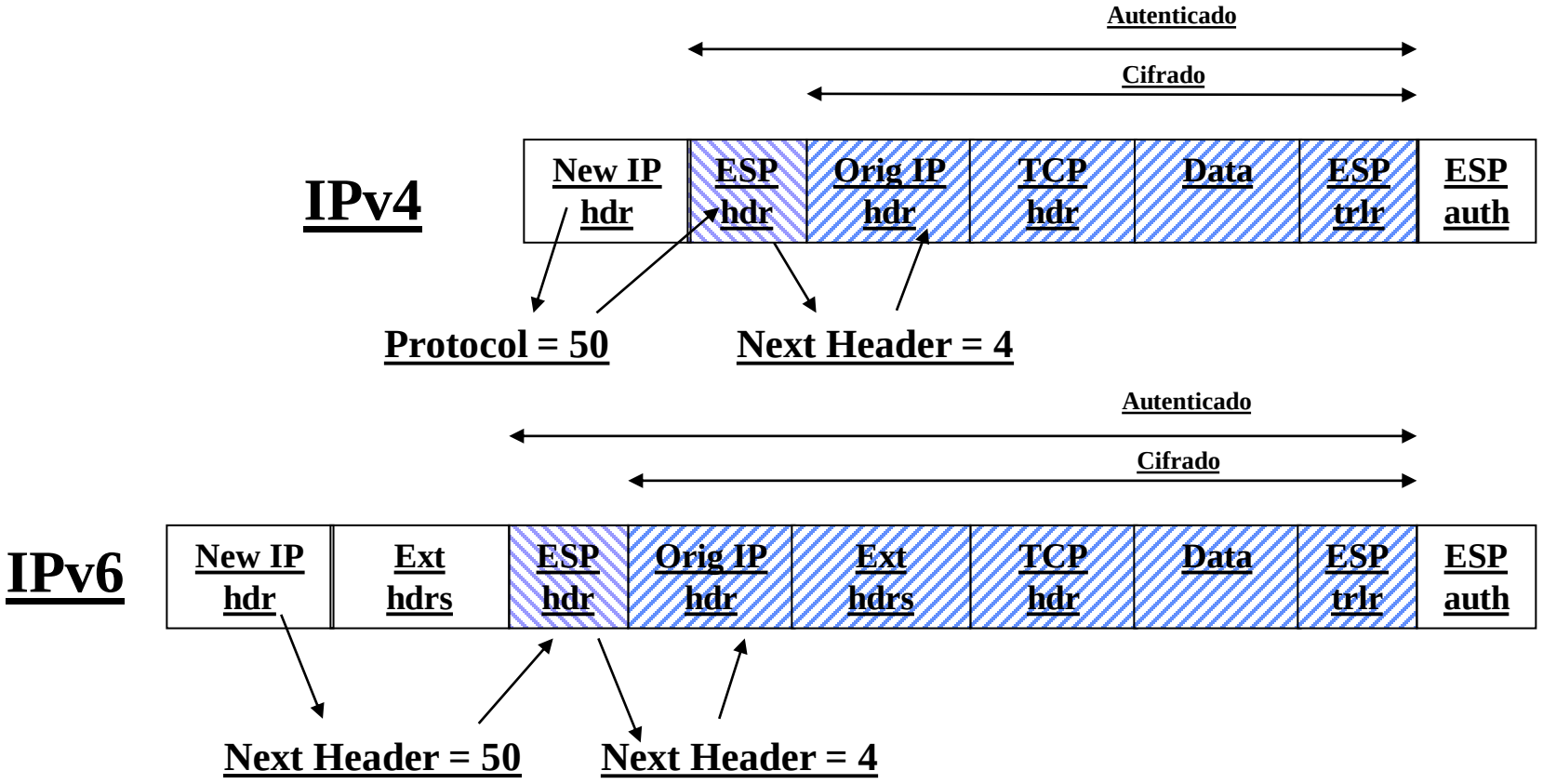
Encapsulating Security Payload (ESP): RFC 4303

- Número de protocolo IP: 50
- Autenticação ESP é opcional mas é usada muitas vezes em vez do AH
- O cabeçalho IP original é cifrado

ESP – Modo transporte



ESP – Modo túnel



Padding?

- Estende o texto em claro para um múltiplo de um certo número de bytes para acomodar os algoritmos de cifra (e.g. DES) que necessitam de blocos de dimensão fixa.

- Assegura que o fim do campo Next Header está alinhado à direita com palavras de 32-bit.

- Pode ser negociado de forma a ser utilizado para fornecer confidencialidade parcial de fluxo de tráfego, escondendo a dimensão da carga dos datagramas IP.

Gestão

- A gestão do IPsec deve incluir forma de especificar:
  - Quais os serviços de segurança a usar e em que combinação
  - A granularidade com que determinada protecção de segurança deve ser aplicada
  - Os algoritmos criptográficos a usar para efectuar a segurança

- Dado o IPsec ter necessidade de utilização de chaves criptográficas partilhadas recorre a diferentes conjuntos de mecanismos para a sua distribuição. Pode utilizar distribuição de chaves manual e automática.

- Especifica uma forma de gestão automática de chaves (IKE), mas podem ser utilizadas outros processos automáticos como, por exemplo, o Kerberos.

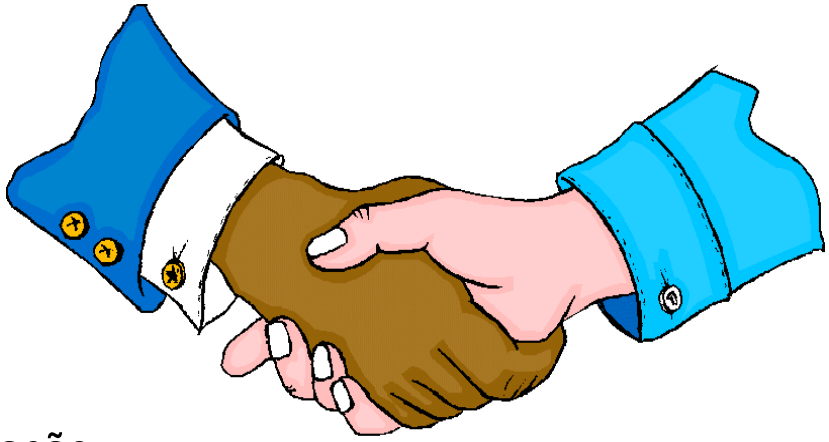
Gestão de chaves

- O IPsec é um grande consumidor de chaves simétricas:
  - Uma chave para cada SA.
  - SA diferentes para:

    {ESP,AH} x {túnel, transporte} x {*sender, receiver*}.
- De onde vêm todos estes SA e respectivas chaves?
- Duas fontes:
  - Chaves manuais.
    - Sem problemas se o número de nós for pequeno mas sem esperança para redes de dimensão razoável com nós conscientes do IPsec; requer rechaveamento manual e lida mal com PFS (*Perfect Forward Secrecy*).
  - IKE: *Internet Key Exchange*, RFC 4306
    - O IKE é uma adaptação específica de protocolos mais gerais (“Oakley” e “ISAKMP”).
    - Os protocolos têm muitas opções e parâmetros.

Associação de Segurança [*Security Association*] (SA)

- Toda a informação partilhada entre dois sistemas IPsec para estabelecer uma ligação segura
  - Selecção dos mecanismos de segurança:
    - Protecção ESP ou AH
    - Modo transporte ou túnel
    - Algoritmo de cifra
    - Algoritmos para a autenticação
  - Autenticação das duas partes
  - Escolha das chaves de cifra e de autenticação
  - O IPSec cria pares de SA - um SA para cada extremo de uma ligação unidireccional



Associação de Segurança [*Security Association*] (SA)

- Uma das principais funções do IKE é a criação e manutenção de associações de segurança.

- Um SA é uma relação unidireccional (*simplex*) entre emissor e receptor
  - Especifica um processo criptográfico a ser aplicado a **este** pacote **deste** emissor para **este** receptor.

- Um SA está associado ao AH ou ao ESP, mas não a ambos.
  - Se ambos os protocolos forem usados são necessários dois SA distintos, de cada lado se a ligação for *duplex*.
  - Em cada direcção da ligação são utilizados SA distintos.

- Os SA são mantidos na **base de dados de SA** (**SAD**)
  - Lista de SA activos

Associação de Segurança [*Security Association*] (SA)

- Cada SA é identificado por um **SPI** (*Security Parameter Index*) único (valor a 32 bits transportado nos *headers* AH e ESP), podendo ainda utilizar-se o **endereço IP de destino** e o **identificador do protocolo de segurança** utilizado (AH ou ESP).
  - O SPI permite ao receptor determinar como processar o datagrama acabado de chegar.
- O conjunto de serviços oferecido por um SA depende do protocolo de segurança seleccionado, do modo, dos pontos de finalização (*endpoints*) e da escolha de serviços opcionais dentro do protocolo.

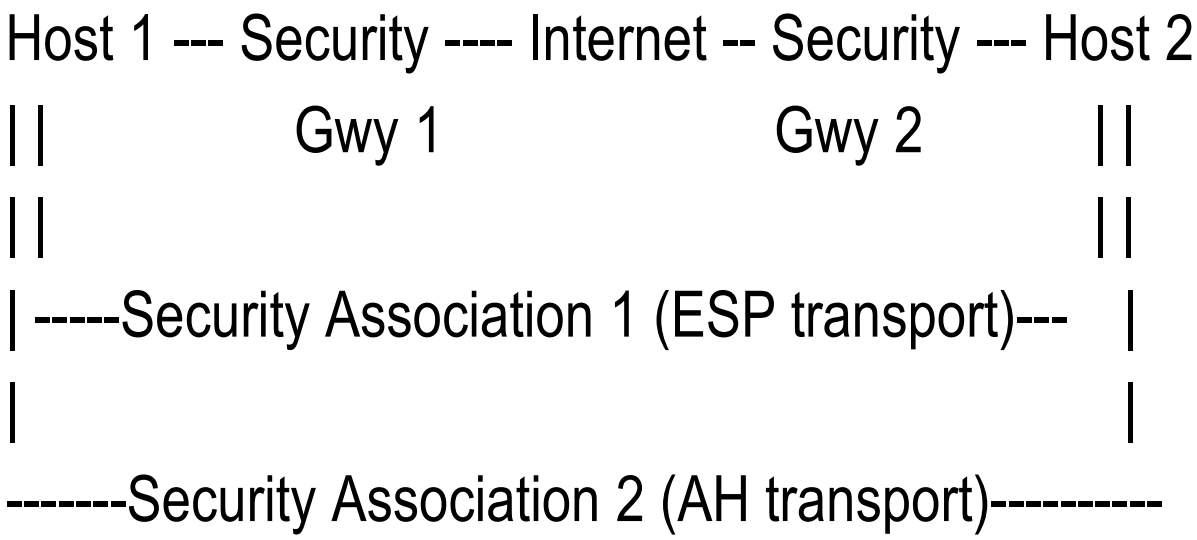
Combinação de SA

- **O RFC 4301 retirou a obrigatoriedade referida no RFC 2401 no que respeita ao suporte de combinações de SA.**

- Muitas vezes, queremos serviços de segurança fornecidos pelo ESP e pelo AH e pretendemos fornecê-los em diferentes sítios da rede.
  - O ESP apenas permite autenticação depois da cifra, podemos pretender o contrário.
- Os SA podem ser combinados usando quer:
  - **Adjacência de transporte (*Transport adjacency*)**: Mais do que um SA aplicado ao mesmo datagrama IP sem túnel
    - Essencialmente AH + ESP.
  - **Túneis iterativos (*Iterated tunnelling*)**: Múltiplos níveis de encadeamento de túneis IPsec; cada nível com o seu próprio SA.
    - Cada túnel pode começar/terminar em diferentes sítios IPsec ao longo do caminho.

SA - Adjacência no transporte

- A adjacência no transporte refere-se a **aplicar mais de um protocolo de segurança ao mesmo datagrama IP**.

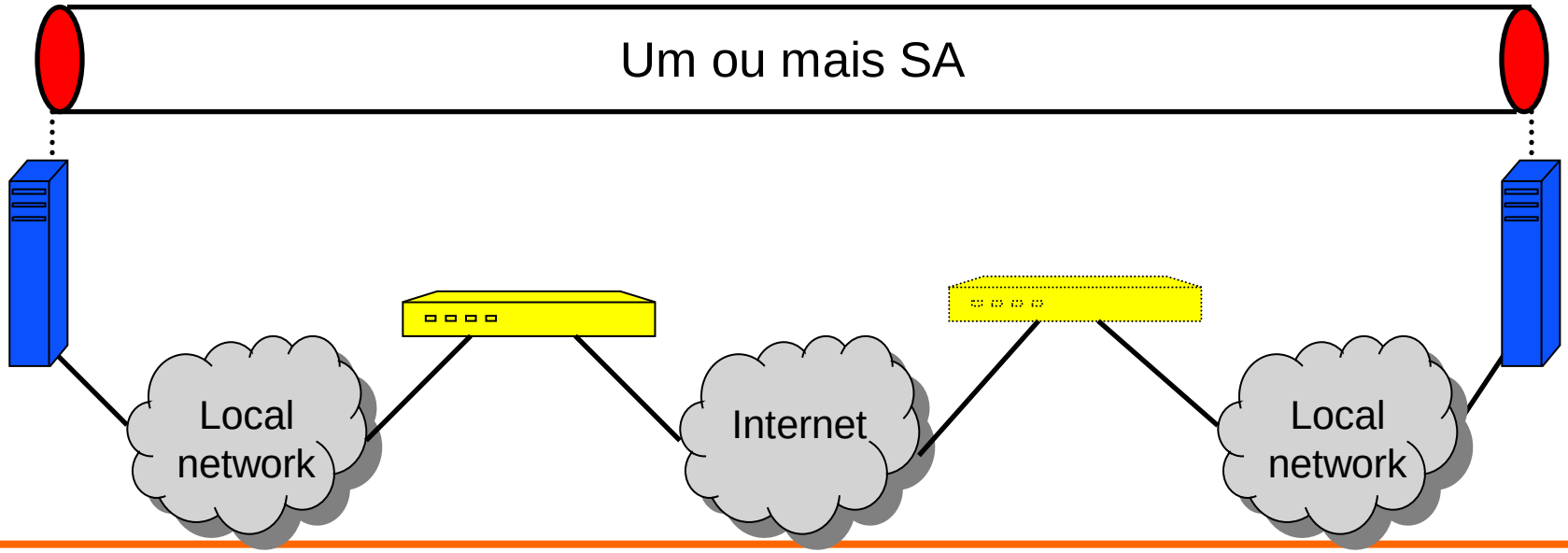


SA – Túnel iterado

- Aplicação de **múltiplos protocolos de segurança ao longo dos túneis**.
- Permite que **múltiplos níveis de encapsulamento** (túneis dentro de túneis), dado que cada túnel pode originar ou terminar em diferentes locais IPsec (*gateways* de segurança) ao longo do caminho e utilizar qualquer dos protocolos de segurança (AH ou ESP).

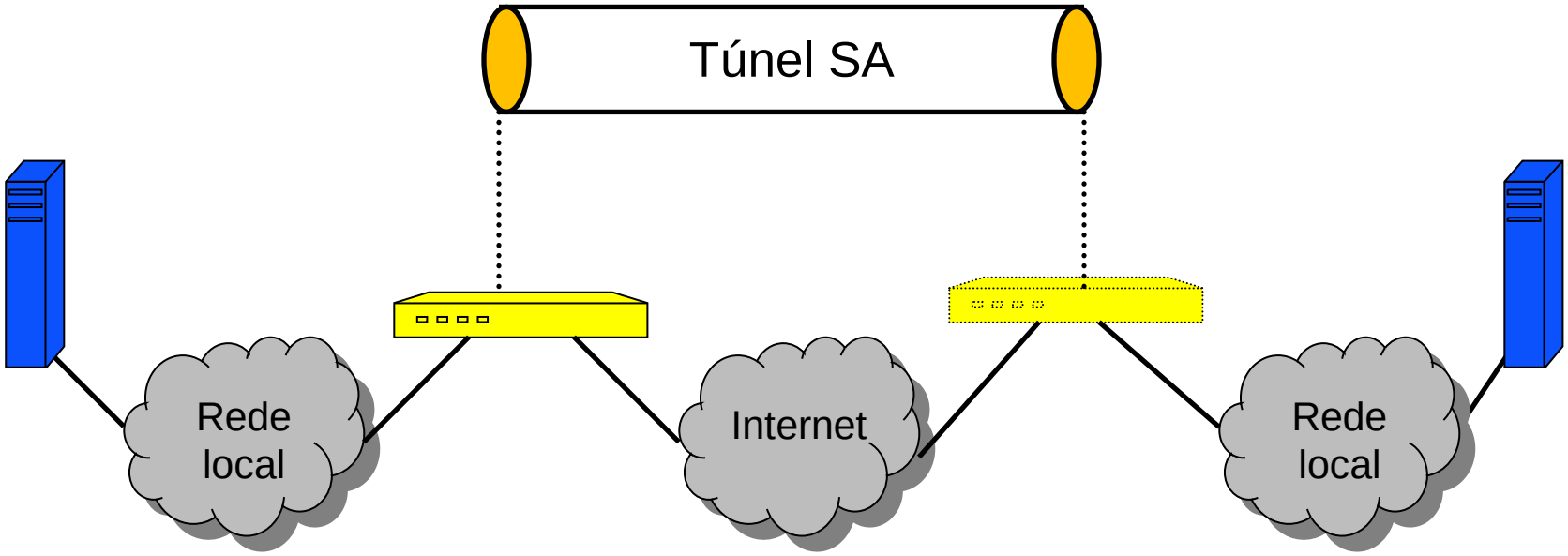
Combinações de SAs

1. Aplicação extrêmo-a-extrêmo de IPsec entre *hosts* conscientes do IPsec (*IPsec-aware*):
   - Um ou mais SA, numa das seguintes combinações:
     - AH no transporte
     - ESP no transporte
     - AH seguido de ESP, ambos no transporte
     - Qualquer dos acima, em túnel dentro de AH ou ESP



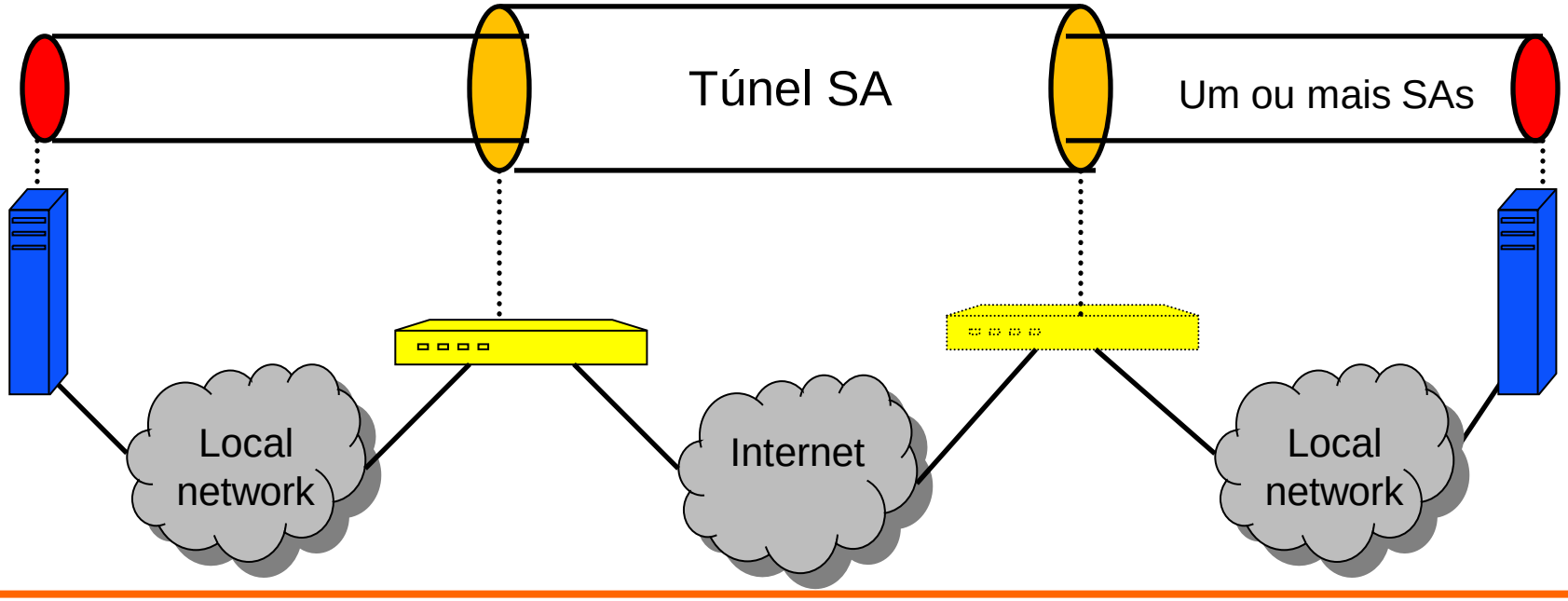
Combinações de SA

2. Apenas *gateway-to-gateway*:
   - Sem IPsec nos *hosts*.
   - *Virtual Private Network* (VPN) simples.
   - SA dum túnel simples suportando qualquer AH, ESP (apenas confidencialidade) ou ESP (confidencialidade+autenticação).



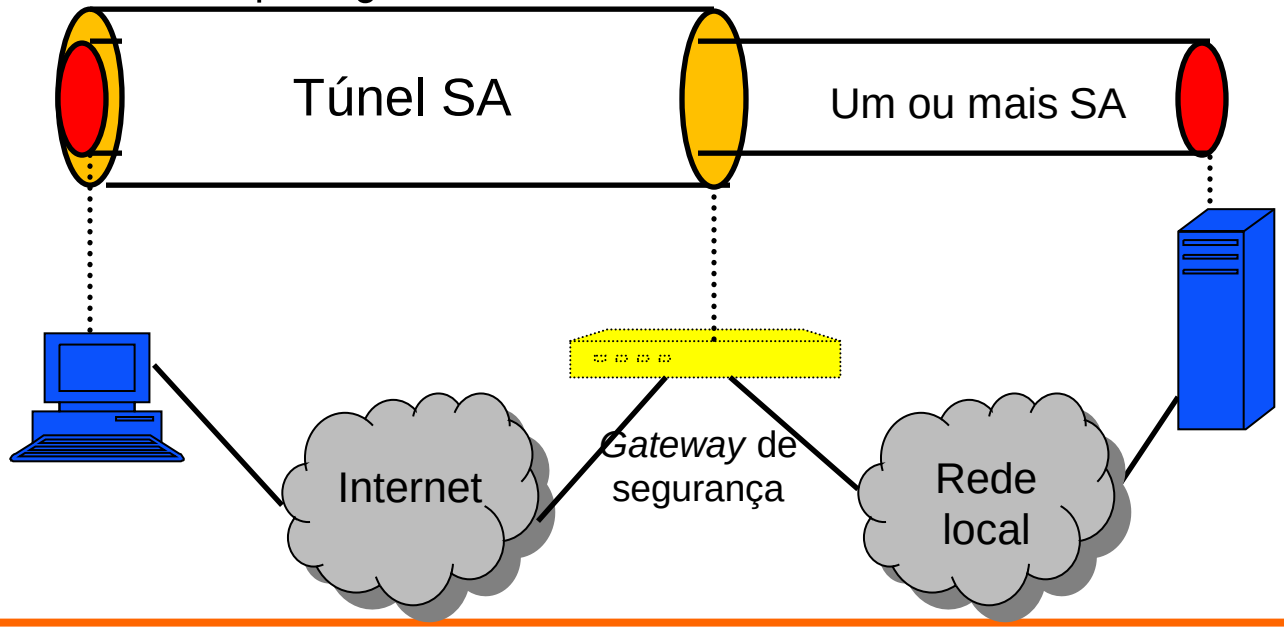
Combinações de SA

3. Combinação do 1 e 2 anteriores:
   - Túnel *gateway-to-gateway* como em 2 transportando tráfego *host*-a-*host* como em 1.
   - Fornece segurança flexível adicional em redes locais (entre *gateways* e *hosts*)
   - E.g., ESP em modo túnel transportando AH em modo transporte.



Combinações de SA

4. Suporte de *hosts* remotos:
   - *Gateway* único (tipicamente um *firewall*).
   - *Hosts* remotos usam a Internet para atingir o *firewall*, ganha então acesso ao servidor para lá do *firewall.*
   - Tráfego protegido por túnel interior para o servidor como no caso 1 anterior.
   - Túnel exterior protege o túnel interior através da Internet.



Selectores

Podem estar presentes no emissor e determinam qual o SA a que um pacote em particular pertence:

- Endereços IP de origem e destino
- Protocolo, TOS, número dos portos
- User ID do utilizador (a partir do S. Operativo)
- Nível de sensibilidade dos dados

– ...

Exemplo de selectores na Security Policy Database:

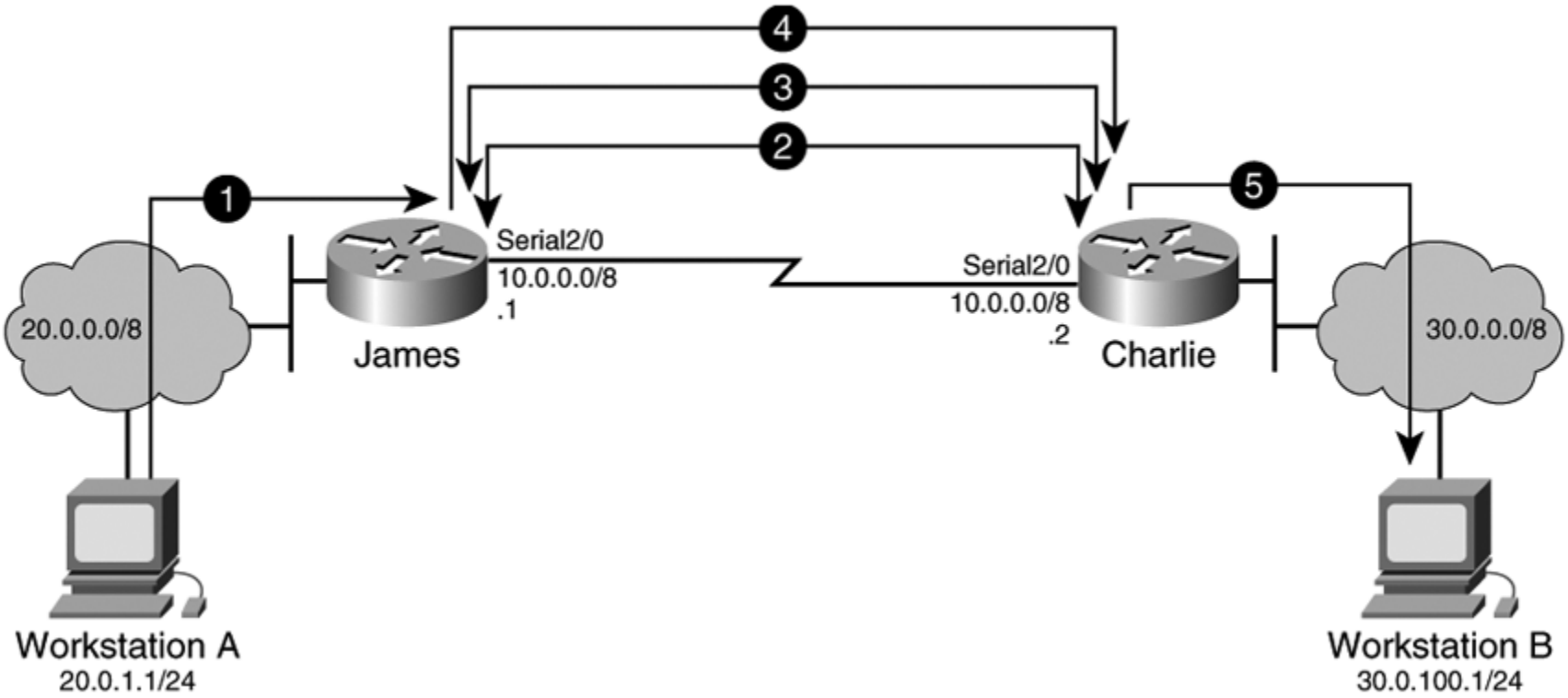
src 192.168.1.20, dest 10.0.0.0/8 port 139, discard # block disk mounts

src 192.168.0.0/16, dest 10.0.0.0/8 port 443, bypass # bypass SSL traffic

src 192.168.0.0/16, dest 10.0.0.0/8 port 80, apply IPsec, SPI=4 # http

src 192.168.0.0/16, dest 10.0.0.0/8 apply IPsec, SPI=5 # all other traffic

Negociação dos SA para o IKE e IPsec



Base de dados de segurança

- ***Security Policy Database* (SPD)**
  - Especifica as politicas que determinam a disposição (*disposition*) de todo o tráfego IP de entrada e saída dos equipamentos.
- ***Security Association Database* (SAD)**
  - Contem os parâmetros que estão associados a cada uma das SA criadas.
- ***Peer Authorization Database* (PAD)**
  - Fornece uma ligação entre um protocolo de gestão de SA (como o IKE) e a SPD.

Cada interface que utiliza IPSec requer bases de dados SPD e SAD separadas em cada sentido, dada a direccionalidade de muitos dos campos que são utilizados como selectores .

Security Policy Database (SPD)

- Uma associação de segurança é uma forma de forçar uma politica de segurança num ambiente IPSec.
- **Especifica quais os serviços e de que forma são oferecidos aos pacotes IP**.
- Contem uma lista ordenada de entradas para politicas de segurança.
  - Cada entrada é apontada por um ou mais selectores que definem o conjunto de tráfego IP coberto por esta entrada para a politica de segurança. Isto define a granularidade das politicas ou os SA.
- A SPD deve ser consultada para todo o tráfego (entrada e saída), incluindo tráfego não IPSec. Pode-se pensar em termos de SPD distintas em cada direcção.

Security Policy Database (SPD)

- Especifica quais os serviços que são oferecidos aos pacotes e de que forma.
- É consultada para o processamento de todo o tráfego de entrada e saída, incluindo tráfego não protegido pelo IPSec, como, por exemplo, do IKE.
- Cada entrada da base de dados de politica de segurança (SPD) inclui:
  - **Selectores**
    - **Endereço IP destino**
    - **Endereço IP de origem**
    - **Nome** (User ID : DNS name, X500 distinguished name, or System Name : host name, X500 distinguished/general name)
    - **Protocolo da camada de transporte (número do protocolo)**
    - **Portas de origem e de destino**
  - **A SPD define a política a usar com cada pacote a tratar:**
    - **Descarrega o datagrama, deixa passar sem mexer, ou processa-o de acordo com o IPsec**
    - **Para o processamento IPSec:**
      - **Modo e protocolo de segurança**
      - **Serviços fornecidos(anti-repetição, autenticação, cifra)**
      - **Algoritmos (para autenticação e/ou cifra)**
  - ***Link* para um SA activo na SAD (se existir)**
- A SPD é gerida via interface de administração

Selectores

- Devem ser suportados os seguintes parâmetros de selectores para a gestão dos SA:
  - Endereço(s) IP destino (gama de endereços)
  - Endereço(s) IP local (gama de endereços)
  - *Next Layer Protocol*
    - Portos
    - IPv6 *Mobility Header*
    - ICMP *message type*
  - Nome (não é obtido a partir do pacote):
    - *String* com o nome *fully qualified* (*email*), e.g. mozart@foo.bar.com
    - *String* com o nome *fully qualified* (DNS), e.g. foo.bar.com
    - *Distinguished name* segundo o X.500, e.g. C=US, SP=MA, O=BBN, CN= Stephen Kent
    - *Byte string*

Selectores/granularidade

- Um SA (ou conjunto de SA) pode ser aplicado a muitos tipos de tráfego ou a apenas um (*fine-grained* ou *coarse-grained*), dependendo dos selectores utilizados para se definir o conjunto de tráfego para o SA.

- Exemplo:
  - Todo o tráfego entre dois *hosts* pode utilizar o mesmo SA sendo-lhe aplicado um determinado conjunto uniforme de serviços de segurança. Em alternativa, o tráfego entre um par de *hosts* pode ser regulado por múltiplos SA, dependendo da aplicação utilizada (definida no campo *Next Layer Protocol*, nos portos, etc.), com diferentes serviços de segurança oferecidos por diferentes SA.

Security Association Database (SAD)

- Inclui todas as *Security Associations* activas
- Para cada entrada SA, inclui:
  - **Identificador :**
    - **SPI – *Security Parameter Index***
    - **Endereço IP de destino exterior**
    - **Protocolo de segurança**
  - **Parâmetros**
    - **Algoritmo e chaves de autenticação**
    - **Algoritmo e chaves de cifra**
    - **Tempo de vida (segundos ou bytes)**
    - **Modo do protocolo de segurança (túnel ou transporte)**
    - **Serviço anti-réplicas**
    - ***Link* para a politica associada no SPD**

Security Association Database (SAD)

- Existe uma SAD por cada implementação de IPsec em que cada entrada define os parâmetros associados com uma SA.
- Cada SA tem uma entrada na SAD.
- Para processamento do tráfego de saída as entradas são apontadas pelas entradas na SPD.
- Para o tráfego de entrada cada entrada na SAD é indexada por:
  - Tráfego *unicast*
    - SPI
    - SPI e tipo de protocolo IPsec
  - Tráfego *multicast*
    - SPI e endereço destino
    - SPI, endereço destino e endereço de origem

Security Association Database (SAD)

- Os seguintes campos de uma SAD são utilizados para o processamento IPsec:
  - *Security Parameter Index* (SPI)
  - Contador do número de sequência (64 bits, 32 opcional)
  - *Flag* de *overflow* do contador do número de sequência – obriga a renovar o SA evitando o envio de mais datagramas IP ou não. Depende de se usar anti-repetição.
  - Janela anti-repetição – contador a 64 bit e um *bit map* para determinar se um datagrama IP de entrada AH ou ESP é ou não uma repetição
  - Algoritmo de autenticação do AH, chaves, etc.
  - Algoritmo de encriptação do ESP, chaves, etc.
  - Algoritmos combinados do ESP, chaves, etc.
  - Tempo de vida do SA
  - Modo do protocolo IPsec – transporte ou túnel
  - *Stateful fragment checking flag*
  - *Bypass* DF bit (T/F)
  - Valores DSCP
  - MTU do caminho
  - Endereço de origem e destino do *header* do túnel

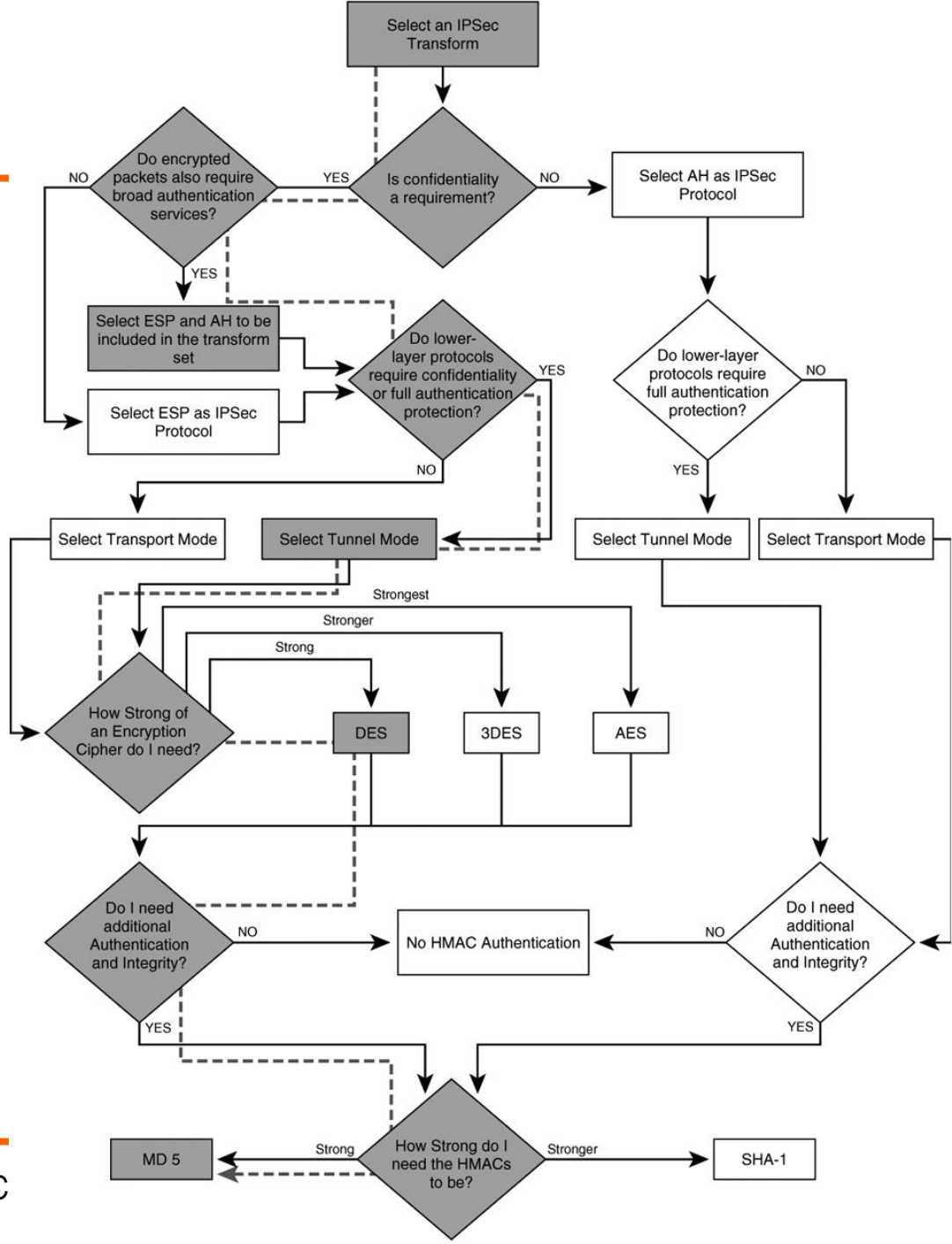
Peer Authentication Database (PAD)

- Entradas na PAD
  - DNS name (especifico ou parcial)
  - *Distinguished Name* (completo ou parcial)
  - RFC 822 *email address* (completo ou parcial)
  - IPv4 *address* (gama)
  - IPv6 *address* (gama)
  - Key ID (exacta)
- Localizada uma entrada após uma pesquisa na PAD baseada no campo ID, é necessário verificar a identidade assumida (autenticação). Por cada entrada na PAD existe a indicação de qual o tipo de autenticação a efectuar. Devem ser suportados:
  - Certificados X.509
  - Segredos pré-partilhados

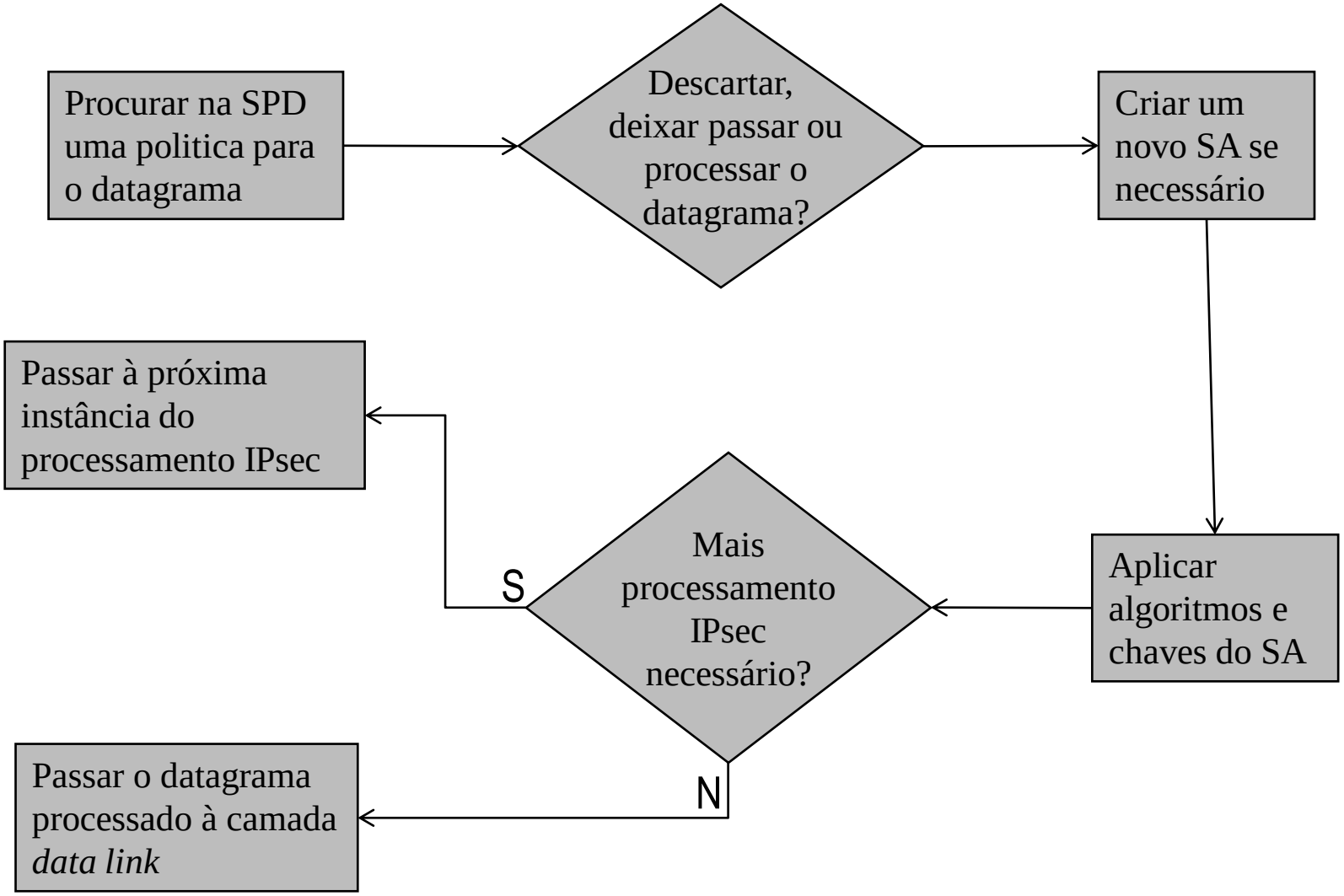
Transformadora IPsec (*IPsec Transform*)

- A transformadora IPsec define uma série de parametros que serão usados para transformar um datagrama de texto em claro para texto cifrado.

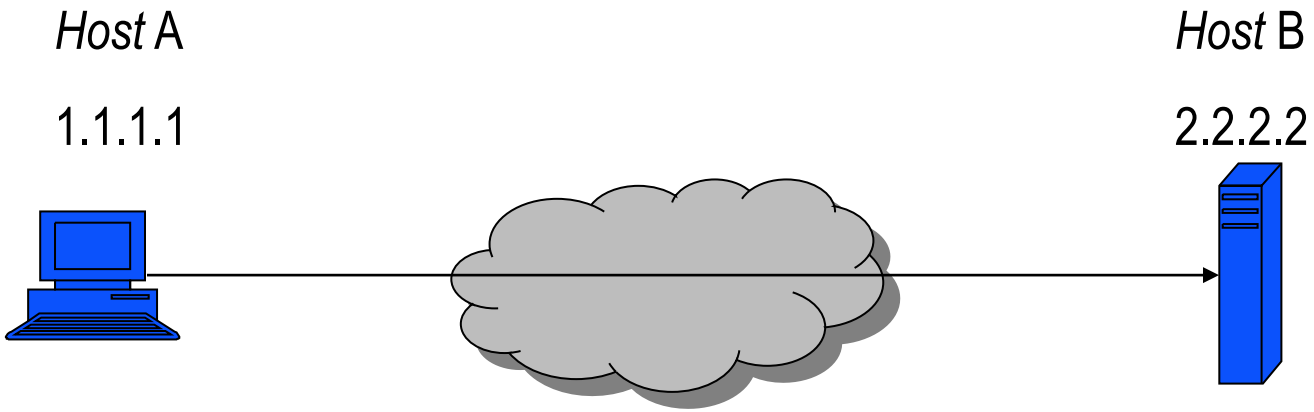
Árvore de decisão de criação de uma “transformadora”



Processamento no envio (*outbound*)



SPD e SA em acção



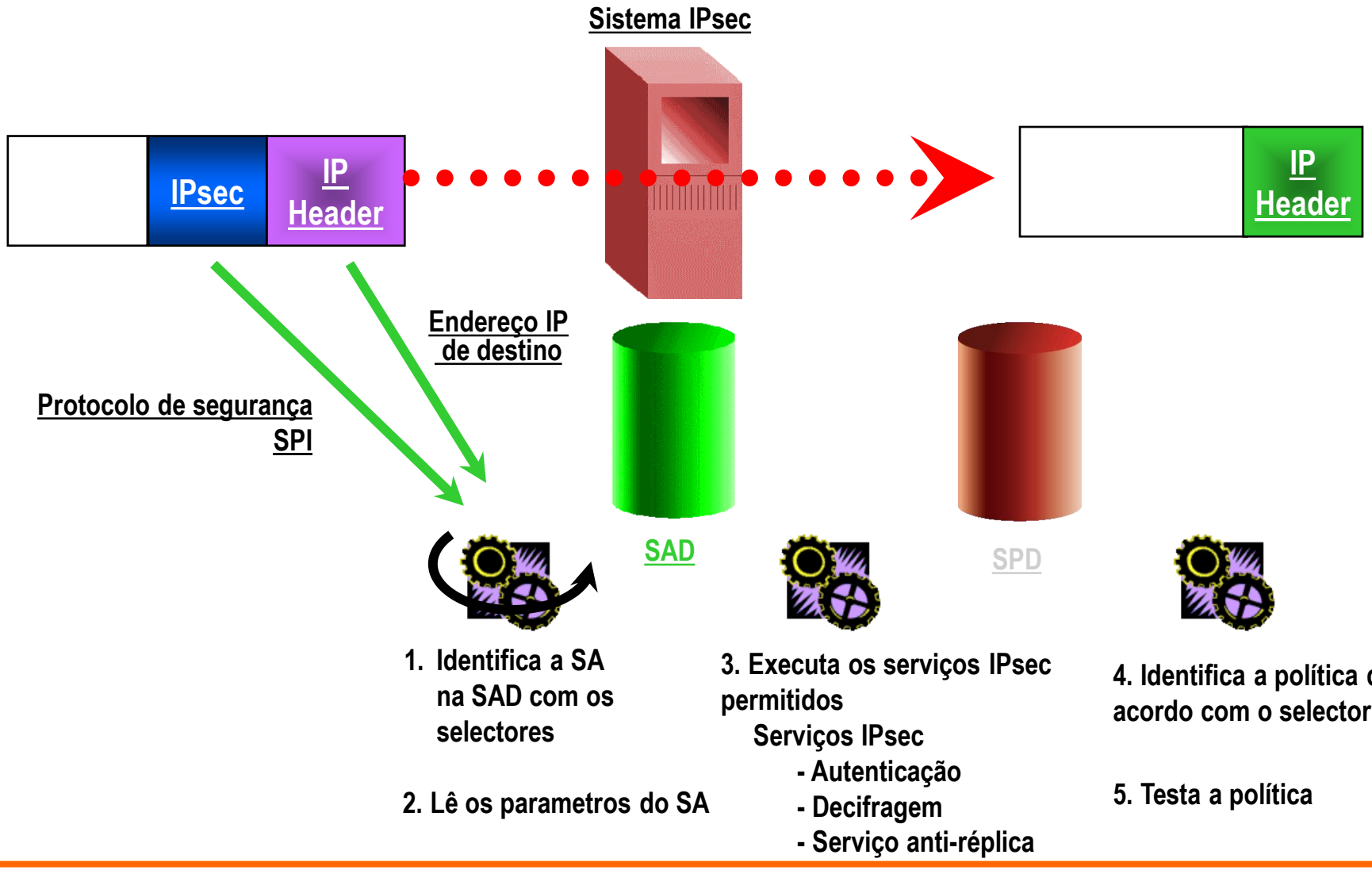
SPD de A:

De	Para	Protocolo	Porto	Politica
1.1.1.1	2.2.2.2	TCP	80	Transporte ESP com 3DES

SAD de saída de A:

De	Para	Protocolo	SPI	SA *record*
1.1.1.1	2.2.2.2	ESP	10	Chave 3DES

Processamento dum pacote de entrada



Janela anti-repetição

Quando uma SA é estabelecida, o emissor inicializa a zero um contador a 64 bits (32 bits no IKEv1) e incrementa-o de 1 por cada pacote enviado.

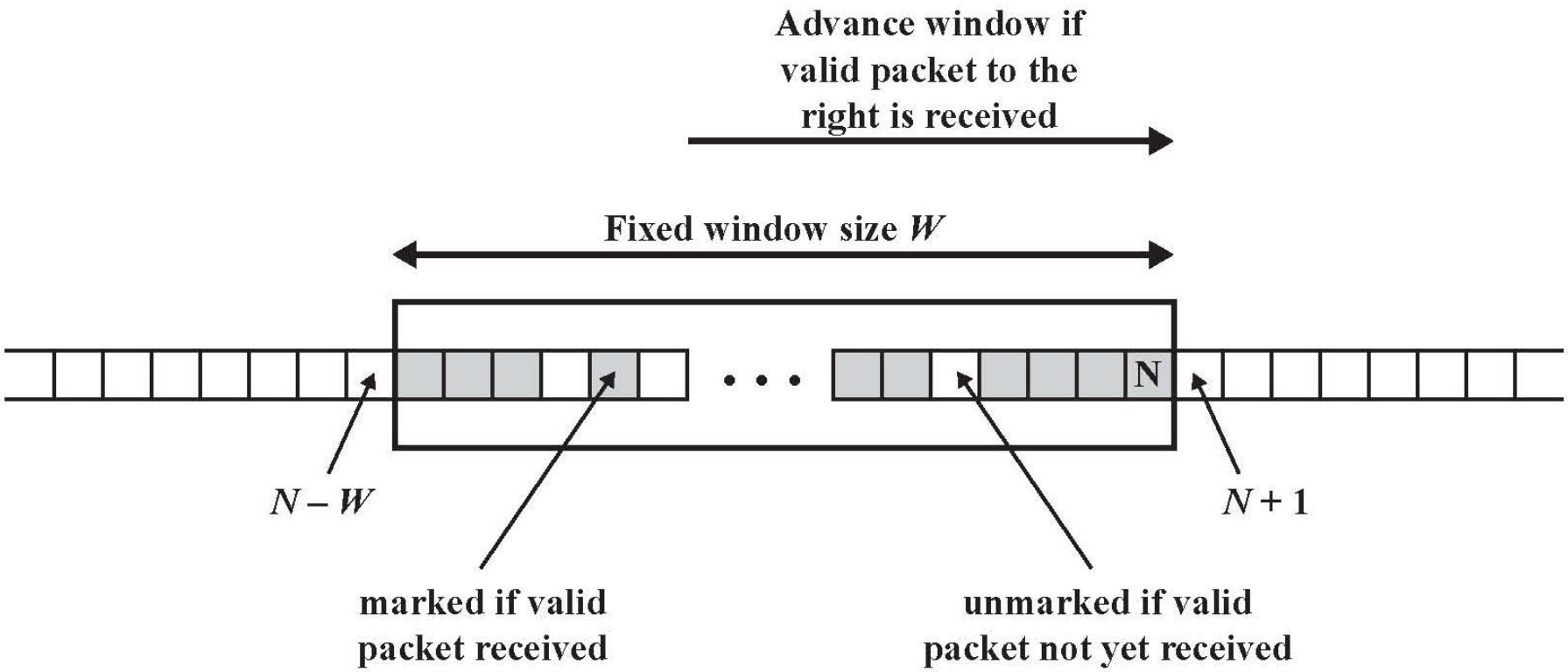
- Este valor servirá como número de sequência
- Se der a volta (2^{64}-1) deve ser estabelecido um novo SA (para protecção anti-repetição).

- Nos **pacotes IPSec apenas é enviado o valor dos 32 bits de menor peso** embora a autenticação seja realizada com o valor a 64 bits

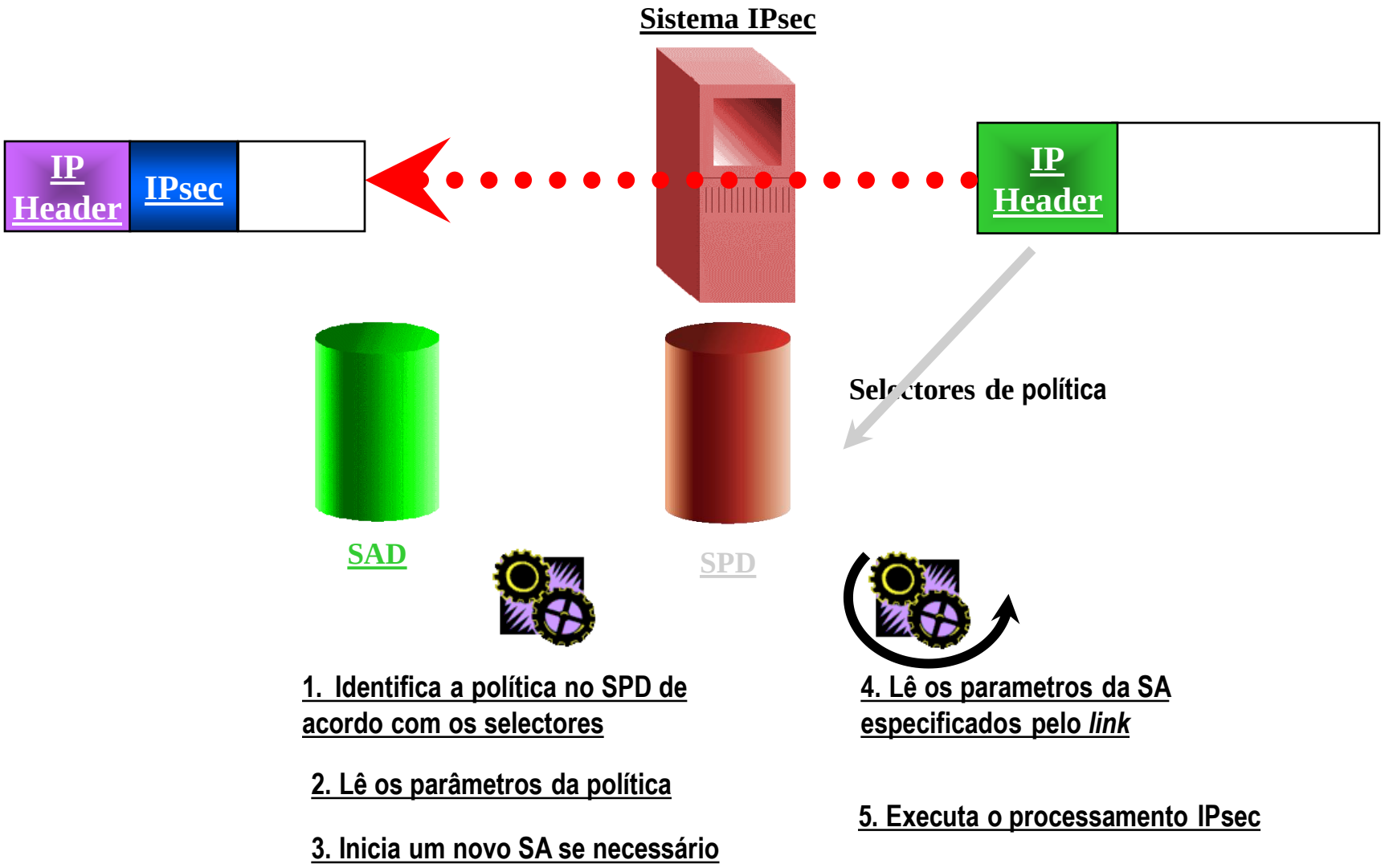
Janela anti-repetição

O receptor mantém uma **janela deslizante de 64 bit**

- Se um pacote com um número de sequência (N+1), superior ao limite superior da janela, for recebido a janela só avança se o pacote fôr autenticado com sucesso.



Processamento dum pacote de saída



Authentication Header - AH

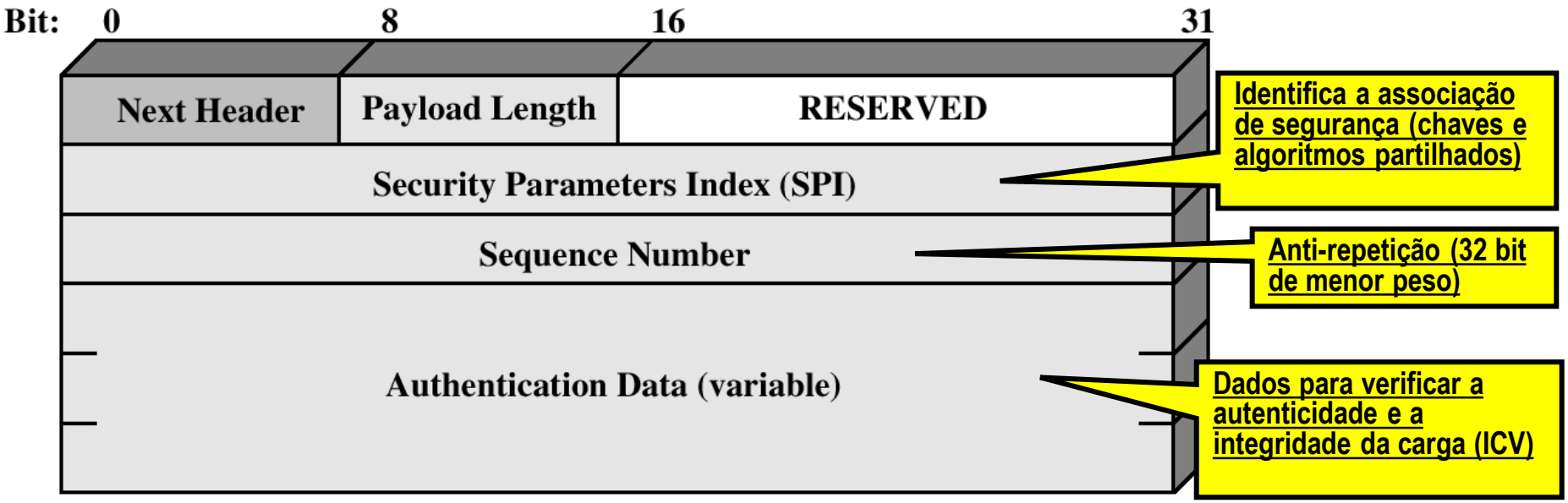
AH

- Foi pensado para oferecer autenticação da origem dos dados, integridade e, opcionalmente, anti-repetição.

- **Algoritmos para autenticação**
  - Algoritmos de cifra simétricos (e.g. AES)
  - HMAC - MD5 – 96
  - HMAC com SHA-1
  - HMAC com SHA-256

Cabeçalho de autenticação

- Fornece suporte para a integridade de dados e autenticação (código MAC) dos pacotes IP.
- Protege de ataques por repetição.



Classificação dos campos IP no protocolo AH

No cálculo do *Integrity Check Value* (ICV), a colocar no campo *Authentication Data* do *header* AH, os campos do *header* do datagrama IP são considerados da seguinte forma:

- **Imutáveis**
  - *Version*
  - *Internet Header Length*
  - *Total Length*
  - *Identification Protocol* (deve ser o valor para o AH.)
  - *Source Address*
  - *Destination Address* (sem *loose* ou *strict source routing*)
- **Mutáveis mas predizíveis**
  - *Destination Address* (com *loose* ou *strict source routing*)
- **Mutáveis** (colocados a zero no cálculo do ICV)
  - *Differentiated Services Code Point* (DSCP) (6 bits, ver RFC 2474
  - *Explicit Congestion Notification* (ECN) (2 bits, ver RFC 3168
  - *Flags*
  - *Fragment Offset*
  - *Time to Live* (TTL)
  - *Header Checksum*

Encapsulating Security Payload - ESP

ESP

- Foi pensado para fornecer o mesmo que o AH, na maioria dos contextos, e confidencialidade.

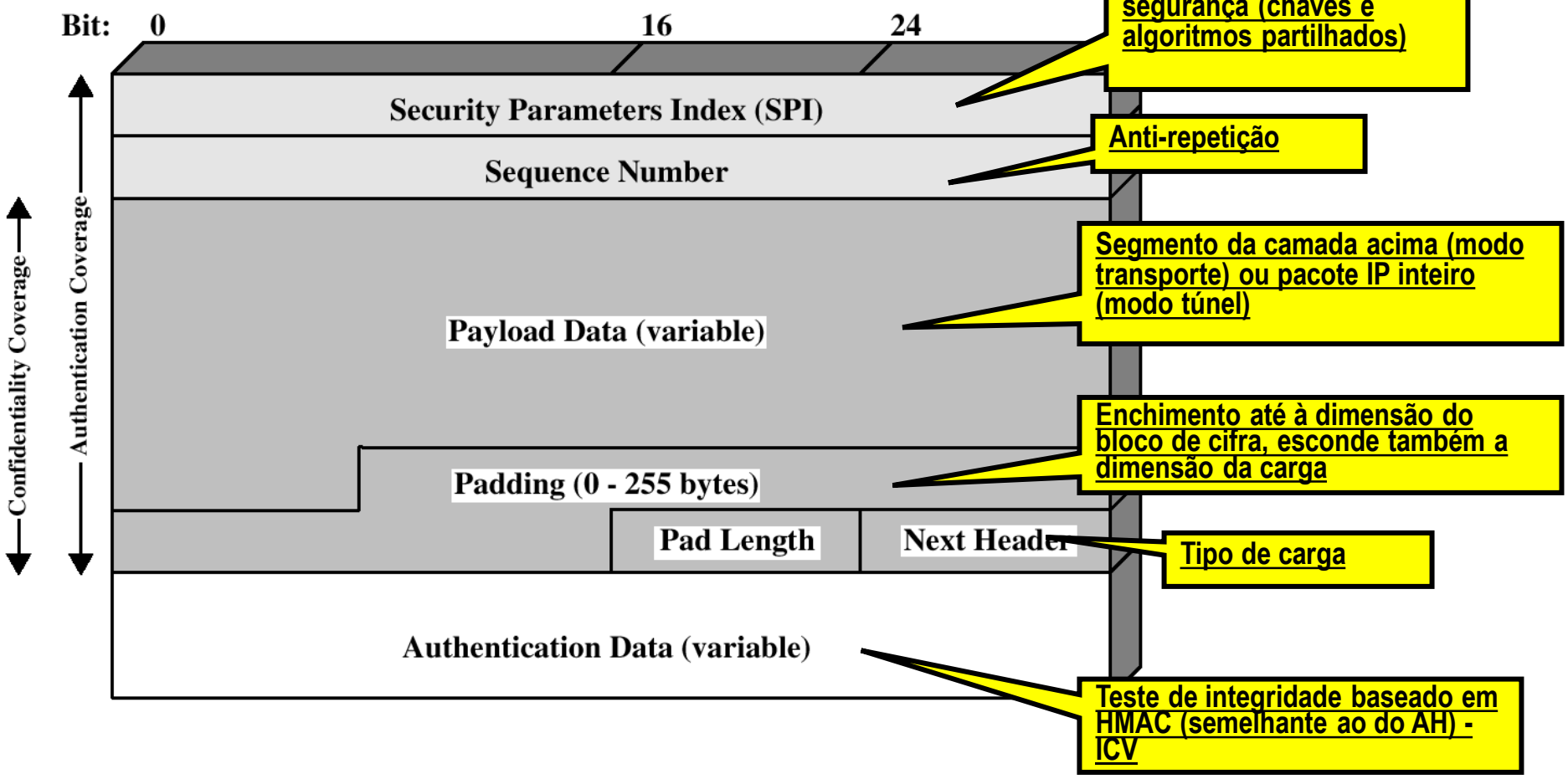
- O ESP DEVE e o AH PODE ser implementado no IPsec.

- Quer o AH, quer o ESP, oferecem controlo de acessos através da obrigatoriedade de conhecimento das chaves ou via certificados digitais.

Algoritmos no ESP

- **Cifra**
  - NULL
  - TripleDES-CBC [RFC2451]
  - AES-CBC with 128-bit keys [RFC3602]
  - AES-CTR [RFC3686]
  - DES-CBC [RFC2405] (Não deve ser oferecida por falta de segurança)
- **Autenticação**
  - HMAC-SHA1-96 [RFC2404]
  - NULL
  - AES-XCBC-MAC-96 [RFC3566]
  - HMAC-MD5-96 [RFC2403]
- **Combinados**
  - Não há nenhum proposto, AES-CCM em estudo

Encapsulating Security Payload



Compressão

- Pode ser negociada compressão no IPsec – IPComp (RFC 2393)
- Deve ser aplicada antes da cifra (porquê? Pista: Como comprimir valores aleatórios?)
- Várias formas de compressão possíveis:
  - Proprietárias
  - *Deflate* (RFC 2394)
    - Baseada no algoritmo *deflate ZLIB*
  - LZS (RFC 2395)
    - Baseado no algoritmo *Stac Electronics LZS*

FIM