Administração de Sistemas (ASIST)

IPsec

Novembro de 2014

“Internet Protocol Security” (IPsec)

A arquitectura IPsec é constituída por um conjunto de protocolos que têm como objetivo proporcionar segurança aos protocolos de rede IPv4 e IPv6, nomeadamente nos domínios da confidencialidade e autenticação.

As funcionalidades de segurança do IPsec são implementadas entre os nós finais e o processo deve ser transparente para os nós intermédios. Isso pode não ser simples, se todo o pacote IP for encriptado os nós intermédios não podem ler.

Os nós intermédios necessitam de ler e alterar os cabeçalhos IP, por exemplo:

- para encaminharem necessitam de saber o endereço de destino
- cada nó intermédio é suposto decrementar o TTL no cabeçalho do pacote

O cabeçalho IP não pode por isso ser encriptado, mas pode ser feito o seu controlo de integridade/autenticação, desde que sejam excluídos desse controlo os campos que podem ser alterados pelos nós intermédios (“mutable fields”).

Alguns nós intermédios podem ter necessidades adicionais, por exemplo quando efectuam traduções de endereços (NAT).

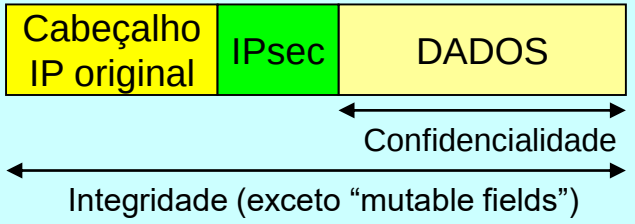
IPsec – modo de transporte e modo de túnel

O IPsec disponibiliza duas formas alternativas de proteger os pacotes IP.

"Transport mode" – o cabeçalho original do pacote mantém-se, a integridade do cabeçalho pode ser garantida (exceto "mutable fields") bem como a confidencialidade e integridade dos dados.

Pacote original

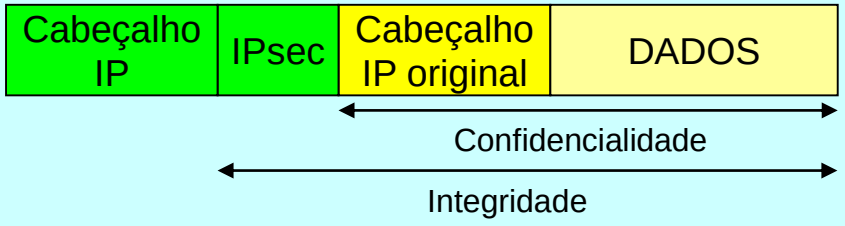
Modo de transporte



"Tunnel mode" – todo o pacote original é transportado no interior de outro pacote (encapsulamento), permite assegurar a confidencialidade e integridade da totalidade do pacote original, cabeçalho incluído. O cabeçalho do pacote exterior pode ser totalmente independente do cabeçalho original

Pacote original

Modo de túnel



IPsec – AH e ESP

Os dois mecanismos mais importantes que o IPsec disponibiliza para implementar a segurança em IPv4/IPv6 são o AH e o ESP.

Tanto o AH como o ESP podem operar em modo de transporte ou modo de túnel:

- IP Authentication Header (AH) – introduz no pacote um cabeçalho adicional que permite garantir a autenticidade, integridade e, dependo dos algoritmos usados, o não repúdio. Não encripta os dados nem o cabeçalho, por isso não garante a confidencialidade.

- IP Encapsulating Security Payload (ESP) – introduz no pacote um cabeçalho e uma cauda entre os quais são transportados os dados. Garante a confidencialidade dos dados e a autenticidade/integridade. Pode também operar apenas com confidencialidade ou apenas com autenticidade/integridade.

Os dois mecanismos podem ser combinados, normalmente usando AH para garantir a integridade/autenticidade e o ESP para garantir a confidencialidade. Todas as implementações IPsec devem suportar ESP, o suporte de AH é opcional.

IPsec – “Security Associations” (SA)

Uma SA é uma ligação “simplex” (apenas num sentido) que transporta tráfego seguro através do AH ou do ESP, para implementar a segurança nos dois sentidos (“duplex”) são necessárias duas SA.

Cada SA apenas pode estar associada a um dos mecanismos, AH ou ESP. Se numa ligação “simplex” for pretendida a utilização simultânea de AH e ESP são necessárias duas SA, uma para cada.

Associados a cada SA estão definidos vários parâmetros, entre outros:

- mecanismo usado, AH ou ESP e modo de funcionamento (transporte ou túnel)
- os algoritmos usados nesses mecanismos para garantir a integridade/autenticação e/ou confidencialidade
- chaves criptográficas
- SPI (“Security Parameters Index”) – número de 32 bits, definido pelo emissor da ligação, que serve para identificar a SA, os cabeçalhos AH e ESP transportam o SPI. O SPI é único para cada endereço de destino.

Em adição ao SPI, no caso de comunicações multicast, a identificação da SA recorre ainda ao endereço IP de origem e endereço IP de destino.

“Security Policy Database” (SPD)

A utilização do IPsec está associada ao controlo de acesso definido na SPD, trata-se de um conjunto de ACLs em que as regras, podem ter três resultados:

- DISCART (DROP/DENY) – o pacote é destruído
- BYPASS – é permitida a passagem do pacote sem aplicação de IPsec
- PROTECT – o pacote é protegido com IPsec, neste caso o SPD especifica os parâmetros de segurança que devem ser usados.

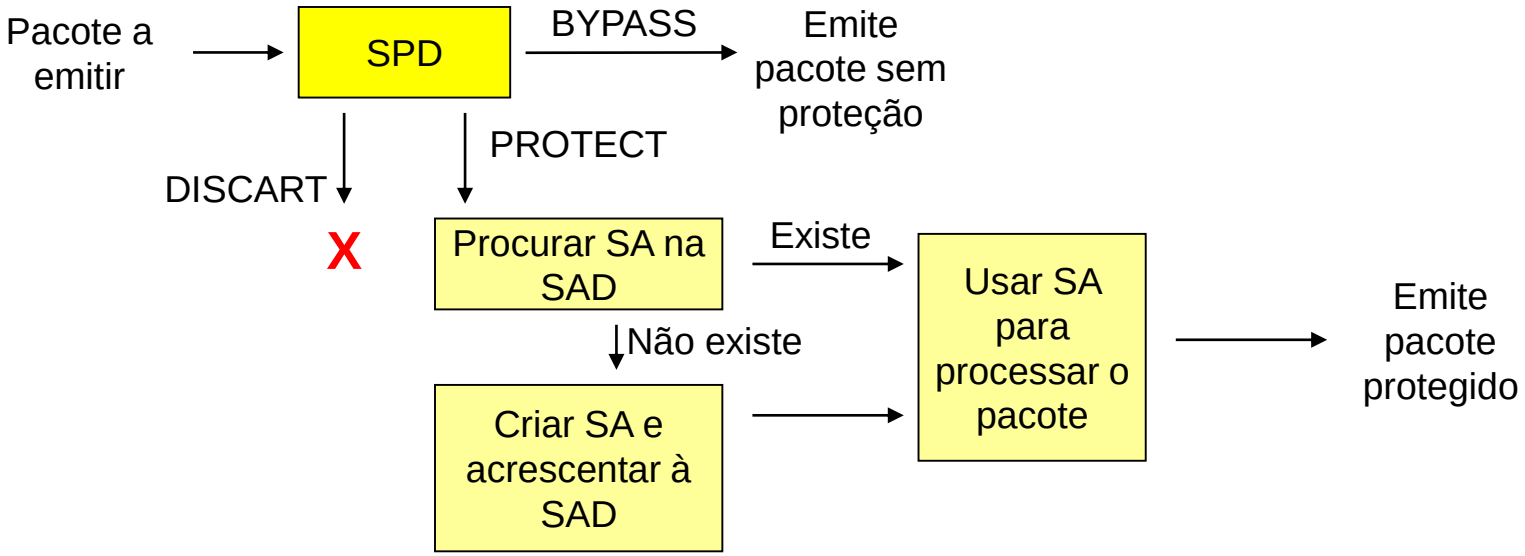
O SPD está dividido em 3 partes lógicas (na prática pode ser uma única ACL):

- SPD-I (“inbound”) – aplica-se ao tráfego de entrada DISCART e BYPASS
- SPD-O (“outbound”) - aplica-se ao tráfego de saída DISCART e BYPASS
- SPD-S (“secure”) – aplica-se a todo o tráfego PROTECT

Na terminologia do SPD os critérios (regras) que permitem definir o tipo de tratamento a dar aos pacotes designam-se “selectors”. Os “selectors” do SPD permitem especificar regras com base nos endereços de origem e destino, protocolo de transporte e se aplicável números de porto. As SPD podem ser definidas dinamicamente no processo de estabelecimento da SA.

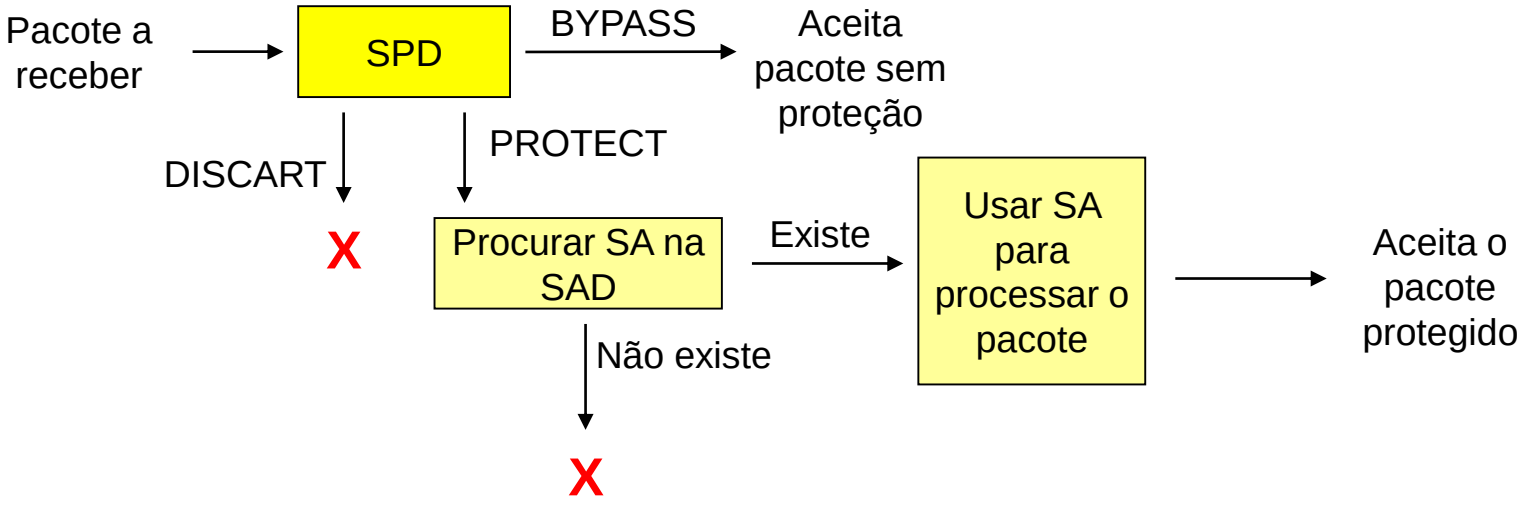
“Security Association Database” (SAD)

Cada nó com implementação IPsec mantém uma base de dados de SA, quando é recebido um pacote para ser processado pelo IPsec, com cabeçalho AH ou ESP o valor do SPI é pesquisado nesta base de dados para determinar os parâmetros que lhe estão associados.



IPsec – receção de pacotes

Um pacote protegido pelo IPsec apenas pode ser recebido com sucesso se a respectiva SA estiver definida na SAD.

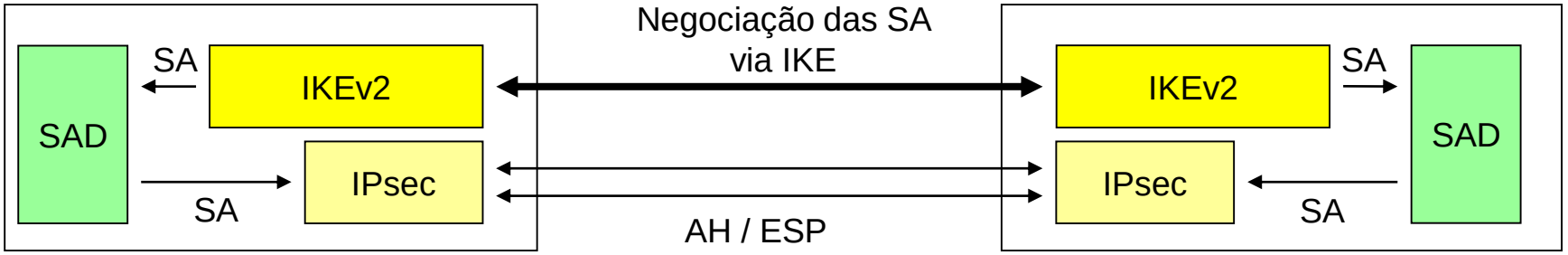


As SA definidas nas SAD são criadas através do “Internet Key Exchange Protocol” (IKE), atualmente IKEv2, o IKE é usado para estabelecer a SA entre dois nós que usam o IPsec, assegura que as SA respetivas, criadas na SAD dos dois nós, são coerentes.

“Internet Key Exchange Protocol” (IKE)

O objetivo do IKE é estabelecer uma SA entre dois nós que implementam o IPsec e permitir que ambos os nós a adicionem às respetivas SAD. Esse objectivo deve ser atingido de forma segura, autenticando os nós e transmitindo a informação de forma confidencial.

O IKE não é a única forma de estabelecer uma SA, a especificação ISAKMP (“Internet Security Association and Key Management Protocol”) é implementada por vários protocolos, entre eles o KINK (“Kerberized Internet Negotiation of Keys”) e o IKE. Atualmente a versão 2 do IKE (IKEv2) é o mais usado.



As implementações IPsec usam o serviço IKE, presente nos dois nós, como auxiliar para negociar e estabelecer uma SA comum que é usada posteriormente pelo IPsec. O serviço IKE é acedido via UDP no número de porto 500, envio e receção.

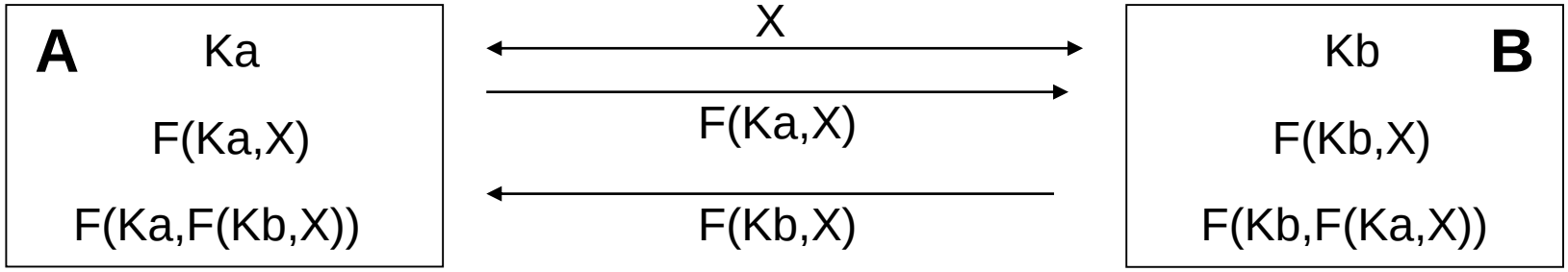
IKEv2

O IKE opera em duas fases:

"Phase 1" – o objectivo é criar uma primeira ligação segura com autenticação, como resultado é estabelecida uma SA especial designada IKE SA.

"Phase 2" – usando a ligação segura através da IKE SA são criadas novas SA.

O algoritmo "Diffie-Hellman" é usado pelo IKE na "phase 1" para criar um segredo partilhado. Tem como base algumas propriedades do algoritmo RSA e permite gerar um valor secreto a partir de dois segredos diferentes (Ka e Kb) detidos pelas duas entidades. De forma simplificada:



O valor X é um número aleatório diferente para cada sessão, as funções F têm propriedades tais que não é possível determinar Ka ou Kb conhecidos F(Ka,X) ou F(Kb,X), no entanto F(Ka,F(Kb,X)) é igual a F(Kb,F(Ka,X)).

IKEv2 – Phase 1

No protocolo IKE original (IKEv1) a “phase 1” podia ser realizada de vários modos, de entre eles o “modo principal” e “modo agressivo”, o segundo modo é mais rápido, mas não protege a identidade dos nós. Em qualquer dos casos é usado o algoritmo “Diffie-Hellman” para produzir um valor secreto designado SKEYSEED que vai ser usado para gerar todas as restantes chaves.

O IKEv2 simplificou a “phase 1”:

IKEv2 - Phase 1 - envolve 2 trocas de informação em cada um dos sentidos:

- o iniciador envia um pedido “IKE_SA_INIT” com uma lista de algoritmos criptográficos suportados e dados do algoritmo “Diffie-Hellman”, o recetor responde selecionando um algoritmo criptográfico dos propostos e respondendo ao algoritmo “Diffie-Hellman”. Nesta altura fica estabelecido o SKEYSEED.

- o iniciador envia um pedido “IKE_AUTH” com dados para autenticação protegidos por chaves geradas do SKEYSEED. O receptor autentica-se também de forma protegida. A autenticação pode recorrer a certificados de chave pública RSA, assinaturas digitais ou chave pré-partilhada (PSK), no caso de ser usada uma PSK (eventualmente derivada de uma “password”) é usado um algoritmo tipo CHAP.

IKEv2 – Phase 2 (“CREATE_CHILD_SA”)

A designação “phase 2” é herdada do IKEv1 no IKEv2 esta operação designa-se “CREATE_CHILD_SA”, permite a qualquer um dos dois nós envolvidos criar uma nova SA após concluída a “phase 1”.

As mensagens “CREATE_CHILD_SA” são protegidas através do IKE SA, o emissor cria um SA e envia ao recetor, o recetor responde, aceitando a nova SA.

Os IKE SA definidos na “phase 1” devem ser renegociados periodicamente para maior segurança, para esse efeito é também usada uma mensagem “CREATE_CHILD_SA”, o IKE SA anterior torna-se inválido e é criado um novo (com novas chaves).

Os SA genéricos, definidos na “phase 2” também devem ser renegociados periodicamente, para esse efeito é novamente usada uma mensagem “CREATE_CHILD_SA”, anulando o SA anterior e criado um novo, com novas chaves.

IPsec - NAT traversal

Os nós intermédios que efectuam tradução de endereços tendem a causar problemas a alguns protocolos, o IPsec é um desses casos. Ao alterar os endereços IP de origem e destino dos pacotes, e em alguns casos os números de porto, tornam a informação incoerente para o IPsec especialmente em modo de transporte. Isto torna definitivamente impossível a utilização do AH.

A tradução de números de porto NAPT (“Network Address Port Translation”) ou PAT (“Port Address Translation”), permitinde que atrás de um único endereço IP sejam escondidos vários nós com endereços privados, apenas é válido para protocolos com números de porto como o UDP ou TCP, não para o IPsec e outros.

O IKEv2 implementa a funcionalidade NAT-transversal (NAT-T) com o objetivo de resolver alguns dos problemas originados pelo NAT. Para o efeito na phase-1 é determinado se existe no caminho algum dispositivo NAT verificando se o endereço IP de origem está a ser alterado.

Nesse caso, se ambos os nós suportam NAT-T todos os pacotes (IKE e ESP) passam a ser colocados dentro de pacotes UDP (encapsulamento) e é usado o número de porto alternativa 4500 (origem e destino), embora neste contexto seja necessário aceitar pacotes com origem diferente, devido ao NAPT.

Referências bibliográficas

[1] Lhamas A. (2010-2011). Aulas Teóricas de ASIST.

(…)