Universidade da Beira Interior
Faculdade de Engenharia
Departamento de Informática

Segurança Informática
Aula 11
Licenciatura em Engenharia Informática
Licenciatura em Informática Web

Computer Security
Lecture 11
Degree in Computer Science and Engineering
Degree in Web Informatics

Sumário
Segurança e criptografia ao nível da camada de rede e de sessão. Discussão dos protocolos *Internet Protocol Security* (IPSec) e *Secure Sockets Layer* / *Transport Layer Security* (SSL / TLS). Redes Privadas Virtuais (*Virtual Private Networks* (VPNs)).

Summary
Security and cryptography at the network and session layers. Discussion of the Internet Protocol Security (IPSec) and Secure Sockets Layer / Transport Layer Security (SSL / TLS) protocols. Virtual Private Networks (VPNs).

1 Criptografia no Ambiente Internet
Cryptography in the Internet Environment

1.1 Requisitos de Segurança Fundamentais para Aplicações Web
Fundamental Security Requirements for Web Applications

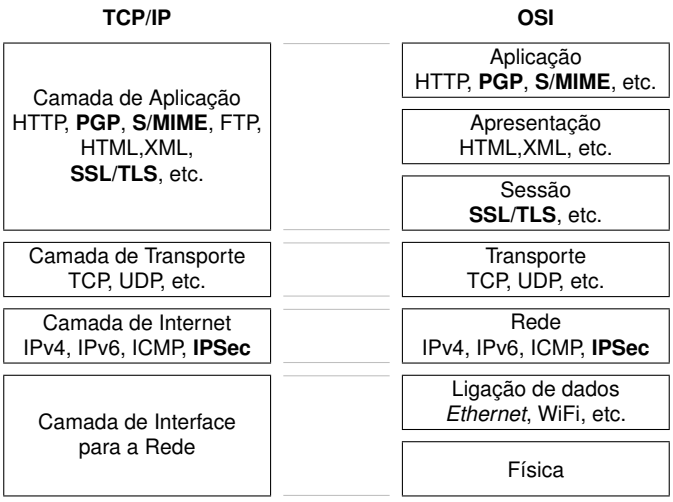
Há **três aspetos fundamentais** a ter em conta quando se desenvolvem soluções de segurança para a Internet:

1. a **autenticação de entidades**, já que estamos potencialmente a operar **remotamente**, sem possibilidade de reconhecer direta e fisicamente pelo menos alguns dos intervenientes da comunicação;
2. a **confidencialidade dos dados**, pelo motivo de que estas comunicações dependem potencialmente de uma infrastrutura que os intervenientes da comunicação não controlam nem policiam totalmente;
3. **Gestão e distribuição de chaves ou segredos** de criptografia, porque acabem por ser necessárias devido aos dois aspetos anteriores, e comportam uma dificuldade em qualquer cenário de aplicação.

1.2 Soluções de Segurança em Diferentes Camadas do Modelo OSI
Security Solutions in Different Layers of the OSI Model

As soluções de segurança podem ser **disponibilizadas em diferentes camadas da pilha** de comunicações da Internet. Por exemplo, é possível fornecer serviços de segurança **ao nível dos pacotes IP usando o IPSec**. Neste caso **desaparecem as preocupações em desenvolver soluções de segurança para quaisquer aplicações que corram sobre IPSec**. Contudo, **nalguns casos**, esta solução **não é versátil o suficiente** para ajustar políticas de segurança a aplicações especificas. Assim, pode-se **recorrer a soluções como o** *Secure Sockets Layer*/*Transpor Layer Security* (**SSL**/**TLS**) para colmatar essa falha. Também é possível **incluir a segurança nas próprias aplicações**, aplicações como é o caso do *Secure/Multipurpose Internet Mail Extensions* (S/MIME), *Pretty Good Privacy* (PGP) e do *Secure Electronic Transaction* (SET).

A figura seguinte mostra a localização concetual de alguns dos protocolos mais conhecidos e realça alguns dos que foram referidos em cima a negrito, para os modelos *Transmission Control Protocol* and *Internet Protocol* (TCP/IP) e *Open Systems Interconnection* (OSI).



De qualquer forma, para qualquer uma das camadas antes mencionadas, pode-se adiantar que:

- A **autenticação** pode ser assegurada por mecanismos de criptografia assimétrica, transmissão segura de valores de *hash* ou *Message Authentication Codes* (MACs).
- A **confidencialidade** pode ser assegurada por **ci-**

fras de chave simétrica.

- A **gestão e distribuição de chaves** pode ser conseguida por mecanismos de criptografia assimétrica, nomeadamente Diffie-Hellman, ou simétrica, e.g. via chaves pré-distribuídas. A gestão de chaves é sempre complicada, e agravada no caso de estarmos a usar criptografia assimétrica, em que cada entidade possa ter mais que uma chave pública.

2 Secure Sockets Layer / Transport Layer Security

Secure Sockets Layer / Transport Layer Security

2.1 Introdução e História

Introduction and History

O *Secure Sockets Layer* (SSL) foi originalmente proposto pela Netscape em 1995, que o desenvolveu com a intenção de assegurar ligações autenticadas entre navegadores (*browsers*) e servidores. O SSL fornece **serviços de segurança à camada de transporte** do modelo OSI, i.e., à camada onde **os protocolos *Transmission Control Protocol* (TCP) e *User Datagram Protocol* (UDP) habitam**. Dado que o SSL se posiciona acima do TCP no modelo *Open Systems Interconnection* (OSI), é mais correto dizer que o SSL fornece serviços de segurança ao nível da camada de sessão.

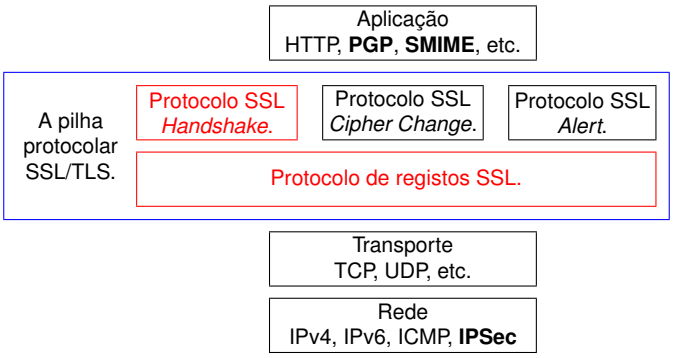
O corpo de trabalho por detrás dos protocolos da Internet, conhecido por ***Internet Engineering Task Force* (IETF)**, fez da **versão 3 do SSL uma norma em 1999** e deu-lhe o nome de ***Transport Layer Security* (TLS) versão 1**. Atualmente, **o SSL vai na versão 3.1 e o TLS na versão 1.2**, estando definida no **RFC 5246**.

Apesar de terem **a mesma filosofia base**, são **diferentes o suficiente para serem incompatíveis**. Contudo, neste capítulo, a expressão SSL / TLS será usada indiscriminadamente para apresentar tanto um como outro.

2.2 Arquitectura SSL/TLS

SSL/TLS Architecture

Na verdade, o SSL/TLS é **composto por vários protocolos** que se podem inserir em **duas camadas do modelo OSI** distintas, conforme se ilustra na figura seguinte.



No esquema incluído antes, há **dois protocolos** que foram realçados a vermelho (o protocolo de aperto de mão e o protocolo de registos), e que serão descritos com um pouco mais de detalhe adiante, dada a sua **importância no contexto do SSL/TLS**.

2.3 Serviços SSL/TLS

SSL/TLS Services

Os **serviços disponibilizados** pelo SSL/TLS são:

1. **Confidencialidade** (através de cifra simétrica);
2. **Autenticação** (principalmente através de criptografia assimétrica) e;
3. **Integridade** e **autenticação da origem dos dados** (através de *Message Authentication Codes* – MACs).

O protocolo permite **3 modelos de autenticação**:

1. **Interações anónimas** (a chave é trocada usando *Diffie-Hellman*).
2. No modelo de **autenticação do servidor**, **o cliente gera uma chave de sessão** e troca-a como servidor usando criptografia assimétrica, nomeadamente através do algoritmo Rivest, Shamir, Adleman (RSA) e **verificando o seu certificado**.
3. No modelo de **autenticação mútua**, **ambos trocam certificados X.509** para se autenticar. O segredo de cifra ou de integridade pode ser **gerado pelo cliente e enviado para o servidor usando criptografia assimétrica**, ou acordado usando Diffie-Hellman.

2.4 Ligação vs. Sessão

SSL/TLS Connection vs. Session

No contexto do SSL/TLS, há **dois conceitos fulcrais** que é necessário entender:

1. O **conceito de ligação** refere-se ao **transporte isolado de uma quantidade de informação** entre dois nós na rede de comunicações. A ligação é, portanto, **uma relação ponto a ponto** entre dois nós, considerada **efémera**. Cada ligação está associada impreterivelmente a uma sessão.
2. O **conceito de sessão** refere-se à **associação duradoura entre um cliente e um servidor**. Esta associação é **criada pelo protocolo de aperto de mão SSL** (*handshaking protocol*). Uma sessão **pode ter múltiplas ligações** e é **caracterizada por um conjunto de parâmetros de segurança** que se

aplicam a todas as ligações dessa sessão. O conceito de sessão **resolve o problema de ter de negociar parâmetros de segurança para cada ligação separada**.

2.5 Estado da Sessão
Session State

O **estado da sessão** SSL é caracterizado pelos seguintes parâmetros:

- **Identificador da sessão**, constituído por uma **sequência de bytes escolhida pelo servidor** para identificar um estado de sessão ativo ou sumarizável.
- **Certificado da entidade**, constituído por um certificado **X.509v3**, que **pode estar vazio** caso se tenha optado por autenticação anónima ou apenas autenticação do servidor.
- **Método de compressão**, constituído por uma variável que **identifica o algoritmo usado para comprimir os dados**.
- ***Cipher Spec***, concretizado numa estrutura ou conjunto de variáveis que **especificam os algoritmos criptográficos** usados no contexto da sessão.
- **Segredo mestre**, constituído por um segredo de 48-bytes partilhado entre o cliente e o servidor.
- Um **booleano** que indica se a sessão **pode ou não ser retomada** (i.e., **se se podem estabelecer mais ligações dentro de determinada sessão**).

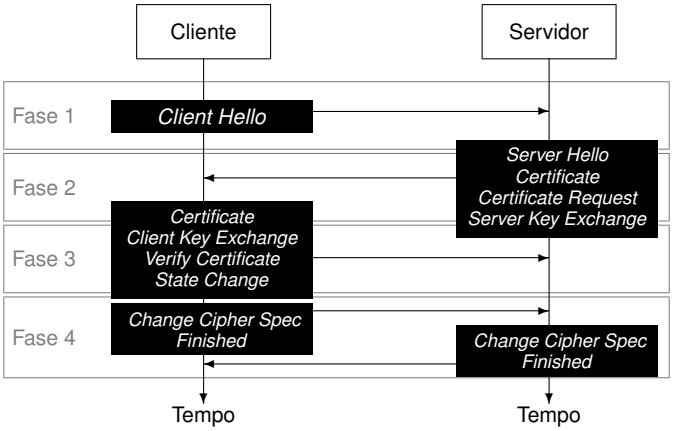
2.6 Estado da Ligação
Connection State

O **estado de uma ligação** SSL é caracterizado pelos seguintes parâmetros:

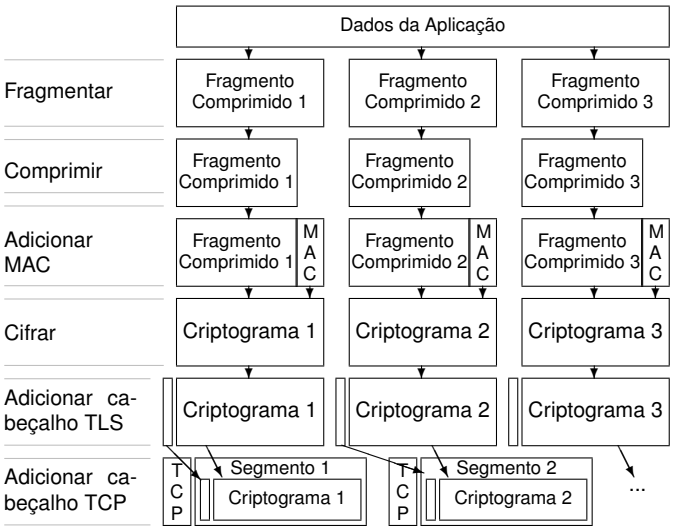
- **Chaves para cifra** do cliente e do servidor, nomeadamente as **chaves simétricas** usadas para cifrar e decifrar dados nos dois sentidos (**uma para cada sentido**).
- **Chaves para cálculo de MACs** para os dois sentidos (**uma para cada sentido**).
- **Vetores de inicialização para cada chave e para cada cifra simétrica por blocos** usada no contexto da ligação. Os vetores são **inicializados durante o protocolo SSL/TLS *Handshake***. Posteriormente, o último criptograma de cada registo é preservado para ser usado como o vetor de inicialização seguinte.
- **Números de sequência**, mantidos isoladamente por cada uma das entidades em comunicação, para efeitos de **contagem e sincronização das mensagens recebidas e transmitidas** durante cada ligação. Quando uma entidade recebe uma mensagem *change cipher spec*, o número de sequência respetivo é reinicializado. Os **números de sequência não podem ultrapassar $2^{64} - 1$.**

2.7 Protocolo de Aperto de Mão
Handshaking Protocol

O **protocolo de aperto de mão** (*the handshake protocol*) é **responsável por autenticar as entidades** em comunicação, **inicializar e sincronizar os estados** das sessões e ligações. É este protocolo que **estabelece as chaves de cifra e de integridade**, e que **negocia os algoritmos** e técnicas usadas pelo protocolo de registos. Esta negociação é esquematizada na figura seguinte.



2.8 Protocolo de Registos
Record Protocol



O **protocolo de registos** é **responsável pela confidencialidade e integridade dos dados**, bem como da **autenticação da origem da informação**. É o protocolo de registos que **transporta os dados do servidor para o cliente e vice-versa**. Para isso, define um procedimento

em que: **(i)** se **fragmentam** os dados em blocos, **(ii)** aplicam primitivas de **autenticação e de cifra** a cada bloco e **(iii)** se entregam esses criptogramas à camada TCP para que sejam transmitidos na rede. Do outro lado, os blocos são decifrados, a sua integridade é verificada, reconstruidos, e entregues à aplicação que os enviou. O fluxo do procedimento que prepara os dados para entrega à camada de transporte encontra-se ilustrado na figura anterior.

2.9 Serviços SSL/TLS
SSL/TLS Services

A combinação do SSL/TLS com outros serviços, protocolos ou aplicações de Internet é normalmente feita notar pela **adição de um S no acrónimo do respetivo protocolo**, e pela **adição da palavra *secure*** no início ou no fim da expansão desse acrónimo, como de resto se demonstra na tabela seguinte:

Protocolo	Porta	Protocolo	Porta
HTTPS	443	IMAPS	991
ftp-data	889	SLDAP	636
SSMTP	465	telnets	992
FTPS	990	SPOP3	995
SNNTP	563	IRCS	993

O *OpenSSL* é uma implementação dos algoritmos (e dos próprios protocolos) do SSL e TLS.

2.10 Ficha Técnica
Technical Sheet

Uma implementação compatível com a versão 1.2 do TLS apresenta a seguinte ficha técnica, em termos de algoritmos usados nos diversos serviços/funcionalidades:

Cifras de Chave Simétrica: AES, DES, 3DES, RC4

Algoritmos de Compressão: ZLIB

Funções de Hash Criptográficas e Esquemas de MAC: MD5, SHA1, SHA256, HMAC.

Protocolos de Acordo de Chaves: Fortezza, Diffie-Hellman, Troca de chaves baseado na cifra RSA.

Esquemas de Assinatura Digital: RSA, Digital Signature Algorithm (DSA).

3 Internet Protocol Security (IPSec)
Internet Protocol Security (IPSec)

3.1 Introdução
Introduction

Uma das formas de implementar segurança na Internet (e de criar Redes Privadas Virtuais) consiste em **fornecer os serviços** de autentificação da origem da informação, confidencialidade e gestão de chaves **ao nível da camada de rede**, nomeadamente **ao nível dos pacotes IP**:

- Quando a segurança é implementada a este nível, **cobre imediatamente todas as aplicações que corram sobre a rede**.
- Torna-se **desnecessário fornecer serviços de segurança em separado** para, e.g., trocas relacionadas com *e-mail*, trocas de dados em bases de dados distribuídas, transferências de ficheiros, etc.

Portanto, **evita-se o peso computacional e o custo de desenvolvimento** nos programas **ao nível da camada de aplicação**.

Note-se que **garantir a autenticação da origem da informação** ao nível da camada IP implica **garantir que a fonte do pacote é, de facto, aquela que é indicada no cabeçalho**, e implica garantir também que **o cabeçalho não foi alterado durante a transmissão**. Estas garantias são providenciadas pela inserção de um cabeçalho designado por cabeçalho de autenticação.

Garantir a confidencialidade a este nível implica **garantir que nenhuma entidade maliciosa que consiga escutar o tráfego IP o consegue ler/perceber**. Esta garantia é fornecida pela inserção de um cabeçalho chamado cabeçalho de encapsulação da carga de segurança.

3.2 Normas IPSec
IPSec Standards

O **IPSec** é uma **especificação para as funcionalidades de segurança ao nível do IP**, que são **nativas à versão 6** do *Internet Protocol* (IPv6)[1]. Estas funcionalidades **também podem**, contudo, ser **usadas na versão 4** desse mesmo protocolo (IPv4).

O IPSec está definido em **três** RFCs principais:

1. **RFC4301** *"Security Architecture for the Internet Protocol,"* **S. Kent**, K. Seo. Dezembro 2005;
2. **RFC4302** ***"IP Authentication Header,"*** S. Kent. Dezembro 2005; e
3. **RFC4303** ***"IP Encapsulating Security Payload (ESP),"*** S. Kent. Dezembro 2005.

Há pelo menos **três tópicos** base que importa discutir no contexto do IPSec:

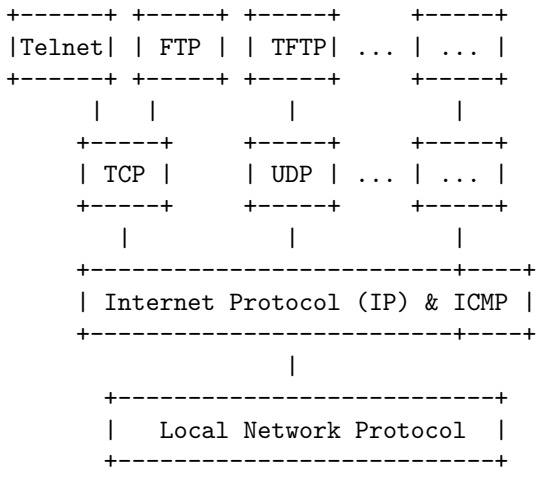
[1] *In addition to the built-in security achieved with IPSec, the main features of IPv6 is its much larger address space. The older and much more widely used IPv4 supports* 4.3×10^9 *addresses, IPv6 supports* 3.4×10^{38} *addresses. (The population of the earth is only (roughly)* 7×10^9*.).*

1. O conceito de associação de segurança (***Security Association*** (SA));
2. Os **dois mecanismos** / **cabeçalhos** que define: (i) o ***Authentication Header* (AH) e o *Encapsulation Security Payload* (ESP)**.
3. Os **dois modos de operação** em que pode funcionar: (i) **Modo túnel** e (ii) **Modo transporte**.

Contudo, antes de prosseguir, convém talvez contextualizar sumariamente o modelo de comunicações sobre IP.

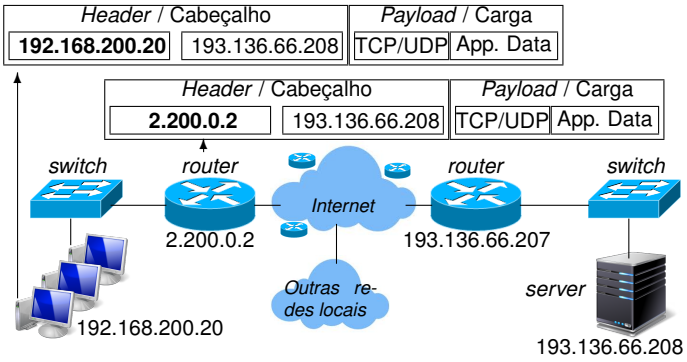
3.3 Comunicações IP
IP Communications

A figura seguinte, adaptada diretamente do RFC que define o protocolo IPv4, com o número 791 e o título *INTERNET PROTOCOL*, ilustra o enquadramento do protocolo mais usado hoje em dia nas comunicações de redes de computadores, em relação a outros protocolos conhecidos:

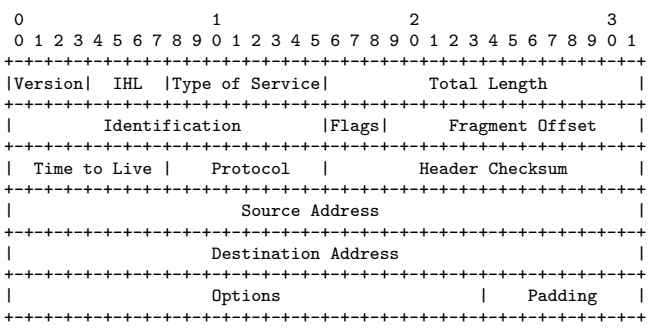


De um modo simplista, pode dizer-se que, **quando uma aplicação pretende transmitir dados para outra aplicação** via rede, **formata-os de acordo com a especificação do protocolo aplicacional** (e.g., *File Transfer Protocol* (FTP)) e **entrega-os ao Sistema Operativo** (SO). O SO **encapsula os dados** num **segmento** *Transmission Control Protocol* (**TCP**) ou num **datagrama** *User Datagram Protocol* (**UDP**), **adicionando-lhes o cabeçalho com as portas** fonte e destino da camada de transporte. De seguida, **o SO adiciona um cabeçalho IP com os endereços lógicos** fonte e destino e uma série de outras informações, construindo assim um pacote IP. Este pacote é **analisado ao longo do caminho em *routers***, que usam a informação no cabeçalho para fazerem chegar essa informação ao destino.

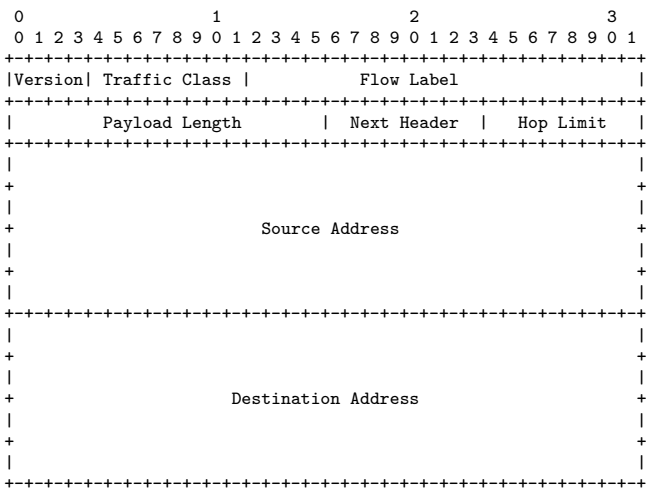
A figura seguinte ilustra, de uma forma muito abstrata, uma pequena parte de uma comunicação IP entre um computador numa rede privada (gama de endereços 192.168.200.0/24) com um servidor. Quando sai do computador da rede privada, o pacote IP leva como destino o endereço IP público do servidor e como endereço fonte o endereço IP do computador dentro da rede de área local. Ao passar pelo primeiro *router*, é aplicado *Network Address Translation* (NAT), e o pacote segue com endereço fonte igual ao IP público associado à interface do *router* que está voltado para a Internet.



De forma a deixar completa esta pequena introdução, ficam ainda as representações dos cabeçalhos IPv4 e IPv6, conforme constam nos RFCs 791 e 2460 (*Internet Protocol, Version 6 (IPv6) Specification*). O cabeçalho **IPv4** esquematiza-se normalmente da seguinte forma:



O cabeçalho **IPv6** esquematiza-se normalmente como se segue:



3.4 Associação de Segurança

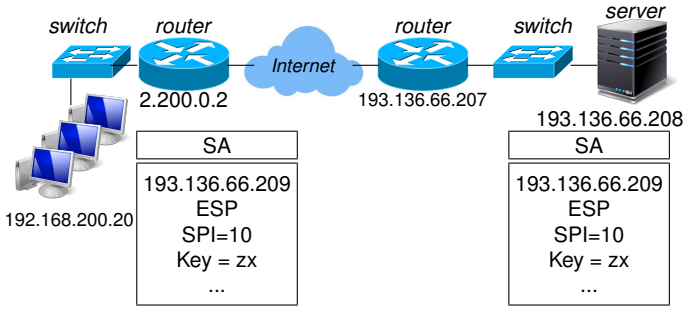
Security Association (SA)

Uma *Security Association* (SA) é um conjunto de regras e parâmetros que indicam como é que uma comunicação segura IPSec entre duas máquinas deve ocorrer. Tem as seguintes particularidades:

- uma SA tem de ser **estabelecida logo no início das comunicações**;
- **indica parâmetros** como chaves de cifra e de autenticação;
- é **unidirecional**, i.e., se quisermos **comunicar nos dois sentidos**, implica criar **2 SAs**;
- e tem **um número de sequência que identifica a SA** chamado *Security Parameter Index* (SPI);

Usam-se protocolos *Internet Key Management Protocol* (IKMP) como o *Internet Key Exchange* (IKE) ou o *Internet Security Association and Key Management Protocol* (ISAKMP) para estabelecimento de SAs.

A figura seguinte, ilustra, de uma forma simplista, o conceito de SA num cenário em que dois computadores comunicam na Internet.



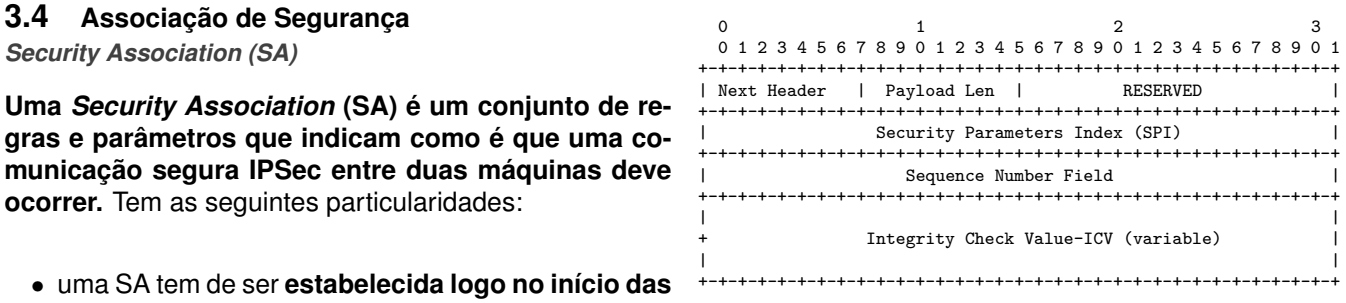
3.5 Cabeçalho de Autenticação

Authentication Header

O mecanismo/cabeçalho *Authentication Header* (AH) serve para **autenticar todo o pacote IP ao qual é acoplado**, **inclusive o cabeçalho extra** que representa. **Autentica a origem da informação (IP) e o conteúdo**. Tal mecanismo é levado a cabo utilizando um *Message Authentication Code* (**MAC**):

1. O **cabeçalho é adicionado ao pacote IP**;
2. O campo do **MAC é inicializado a zeros** (todos os outros são preenchidos normalmente);
3. Calcula-se o MAC e **coloca-se no campo respetivo**.

O cabeçalho AH está definido no RFC 4302 da seguinte forma:



3.6 Cabeçalho de Segurança do Conteúdo Encapsulado

Encapsulation Security Payload (ESP) Header

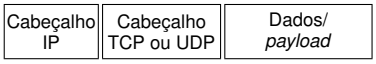
O mecanismo/cabeçalho *Encapsulation Security Payload* (ESP) serve para **cifrar ou garantir a integridade do conteúdo do pacote IP ao qual é acoplado e anexado**. Este mecanismo é assegurado por **um cabeçalho e por um anexo** (expediente) que se juntam ao pacote IP. A confidencialidade é **assegurada por uma cifra de chave simétrica** (normalmente uma cifra por blocos como o AES, pelo que a carga pode ter de ser sujeita a alinhamento (*padding*) antes de ser processada). A integridade é assegurada por um **MAC**. O cabeçalho ESP está definido no RFC 4303 da seguinte forma:

3.7 Modo Transporte

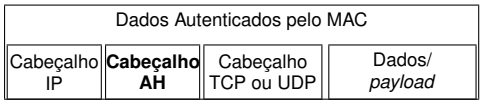
Transport Mode

No modo transporte do IPSec, **o cabeçalho original IPv4 ou IPv6 é mantido**, e **só o conteúdo é alterado de modo a garantir a sua segurança**. **Adiciona-se**, cumulativamente, **um cabeçalho novo depois do cabeçalho IP** e antes do cabeçalho TCP ou UDP que, de resto, tem as informações necessárias para que o pacote passa ser recuperado no outro lado da associação de segurança. O modo de transporte pode ser esquematizado conforme se ilustra a seguir:

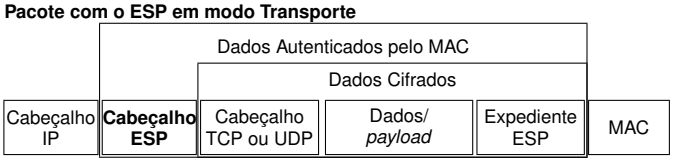
Pacote IP Original



Pacote com o AH em modo Transporte



Pacote com o ESP em modo Transporte

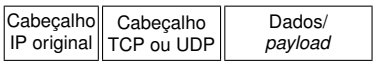


3.8 Modo Túnel

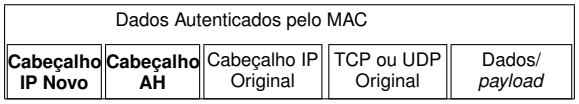
Tunnel Mode

No modo túnel do IPSec, **o pacote IP original é totalmente encapsulado dentro de um novo pacote**, com **novo cabeçalho IPv4 ou IPv6**, ao qual é acoplado o cabeçalho AH ou ESP, conforme se ilustra a seguir:

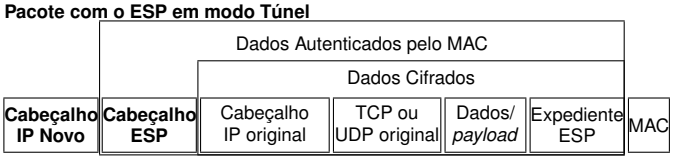
Pacote IP Original



Pacote com o AH em modo Túnel



Pacote com o ESP em modo Túnel



Aquando da **receção** de um pacote IPSec em modo túnel, **o recetor descarta o cabeçalho IP introduzido pelo emissor e recupera o cabeçalho original**. O **cabeçalho exterior serve** assim **para encaminhar pacotes dentro do túnel**, e **o interior serve para os encaminhar para além do túnel**. Por causa disto, este modo é **particularmente útil para criação de Redes Privadas Virtuais**.

4 Redes Privadas Virtuais

Virtual Private Networks (VPNs)

4.1 Definição de Rede Privada Virtual

Virtual Private Network Definition

O conceito de *Virtual Private Network* (VPN) é de extrema importância num mundo onde a mobilidade, a globalização e as redes de comunicação imperam.

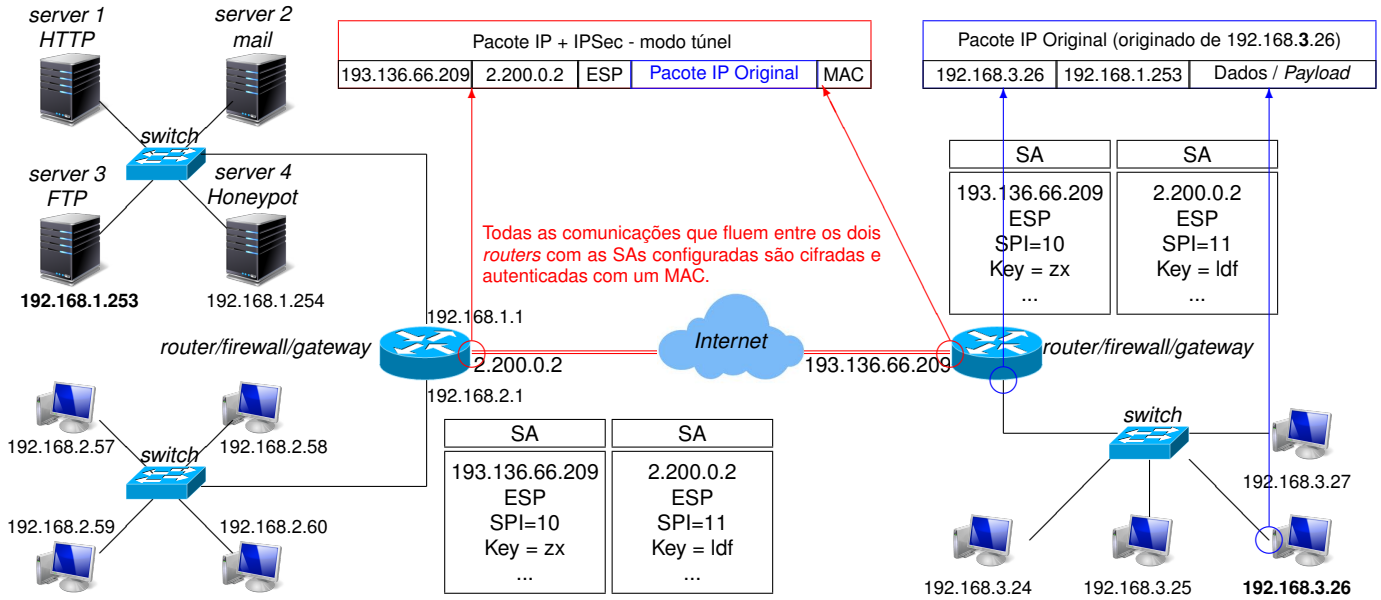
> De um modo genérico, **uma VPN consiste numa extensão segura de uma rede privada**, e.g., organizacional, **sobre uma rede potencialmente insegura**.

I.e., consiste na criação de um ambiente seguro em rede sobre um conjunto de redes que, à partida, podem não ser confiáveis. A implementação de uma VPN pode ser **conseguida à custa da combinação de vários mecanismos de criptografia**. Usando uma VPN, é **possível aceder a serviços internos de uma rede privada, como se estivesse na própria rede**.

4.2 VPN sobre IPSec

VPN over IPSec

Para estabelecer uma **VPN sobre IPSec**, a *gateway* organizacional e o utilizador remoto, ou as duas *gateways* organizacionais têm **ambas de ser compatíveis com IPSec**. Ambas **têm de ter 2 associações de segurança** (para que as comunicações possam ser bidirecionais), com as chaves, algoritmos e mecanismos devidamente sincronizados. Depois de estabelecida a VPN em modo túnel, o utilizador remoto pode aceder ao servidor que está dentro da rede protegida, e que só é cedível dentro da rede protegida (repare-se que o seu endereço IP nem é público). O funcionamento de uma VPN sobre IPSec encontra-se sumaria e parcialmente ilustrada na figura da página seguinte.



Nota: o conteúdo exposto na aula e aqui contido não é (nem deve ser considerado) suficiente para total entendimento do conteúdo programático desta unidade curricular e deve ser complementado com algum empenho e investigação pessoal.