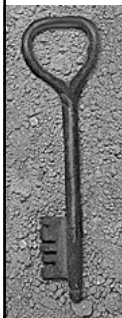


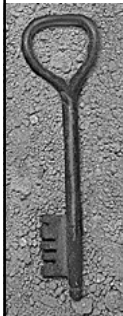


Arquitectura IPsec



Motivação

- ◆ Ainda existem muitas aplicações sem qualquer tipo de segurança
- ◆ Existem protocolos aplicativos específicos de segurança, como o S/MIME, PGP, Kerberos, SSL
 - A sua utilização implica a alteração de software
 - Não é transparente para o utilizador
 - Implica educar os utilizadores
- ◆ Uma solução, implementar a segurança ao nível da camada de rede (IP):
 - Não é necessário alterar *software*
 - É transparente para o utilizador

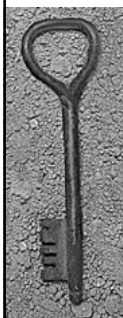


Caracterização (1)

- ♦ Norma de segurança para a Internet, publicado em vários RFC's:
 - RFC 4301 – *Security Architecture for the Internet Protocol*
 - RFC 4302 – *IP Authentication Header*
 - RFC 4303 – *IP Encapsulating Security Payload (ESP)*
 - RFC 2411 – *IP Security Document Roadmap*
- ♦ Um dos autores da RFC 2401 escreveu um livro onde explica detalhadamente o funcionamento do IPSec:
 - N. Deraswamy, D. Harkins, “*IPSec – The New Security Standard for the Internet, Intranets and Virtual Private Networks*”, Prentice Hall, 1999
- ♦ A norma foi criada para o IPv6, mas foi assegurada a compatibilidade para o IPv4

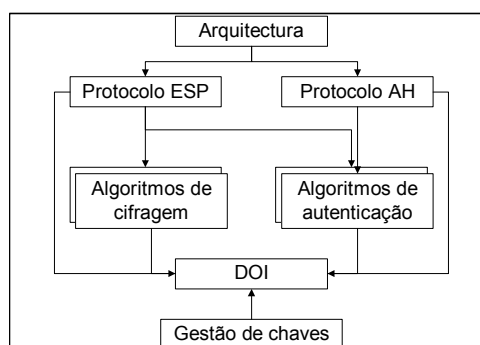
(c) Sílvia Farraposo, Miguel Frade

3



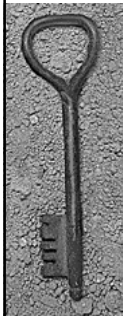
Caracterização (2)

- ♦ Roteiro da documentação IPSec



(c) Sílvia Farraposo, Miguel Frade

4

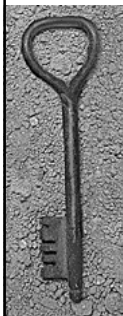


Caracterização (3)

- ♦ O IPSec oferece vários serviços:
 - Autenticação
 - Integridade
 - Anti-replay
 - Confidencialidade
 - Confidencialidade limitada do fluxo
- ♦ Através da definição de dois novos cabeçalhos de extensão ao pacote IP
 - AH (Authentication Header)
 - ESP (Encapsulation Security Payload)

(c) Sílvia Farraposo, Miguel Frade

5

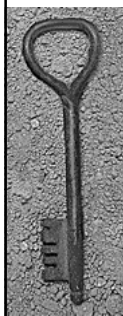


Caracterização (4)

Serviço	AH	ESP	ESP com autenticação
<i>Autenticação</i>	o		o
<i>Integridade</i>	o		o
<i>Anti-replay</i>	o	o	o
<i>Confidencialidade</i>		o	o
<i>Confidencialidade limitada do fluxo</i>		o	o

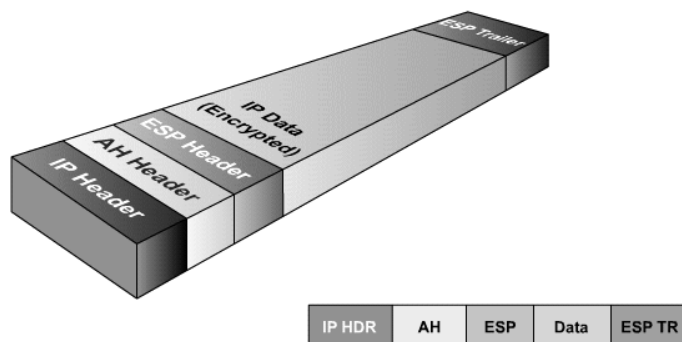
(c) Sílvia Farraposo, Miguel Frade

6



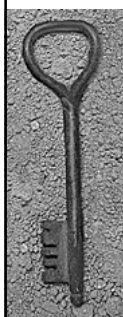
Caracterização (5)

- ♦ Estrutura de um pacote IP com os cabeçalhos de extensão

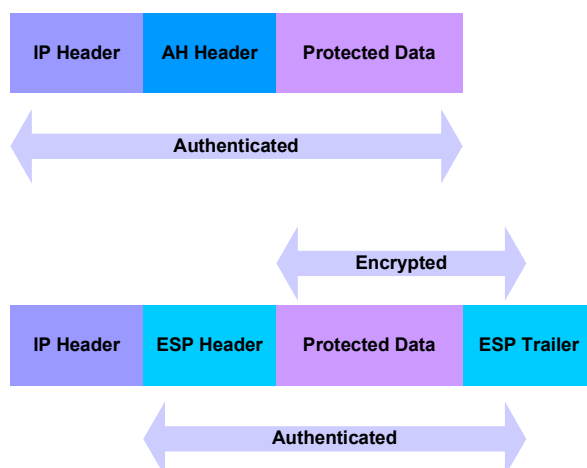


(c) Sílvia Farraposo, Miguel Frade

7

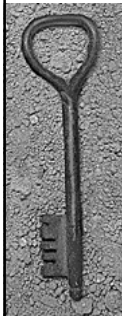


Caracterização (6)



(c) Sílvia Farraposo, Miguel Frade

8

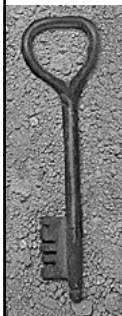


Localização (1)

- ◆ Nos sistemas terminais
 - Segurança extremo-a-extremo
 - Segurança individual de cada fluxo
 - Possibilidade de ligar a SA ao contexto do utilizador
 - Impede a utilização de NAT e IPs privados
 - Duas alternativas
 - No sistema operativo
 - Bump In The Stack (BITS)

(c) Sílvia Farraposo, Miguel Frade

9



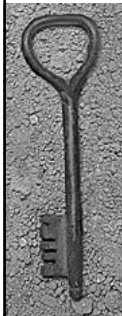
Localização (2)

- ◆ No sistema operativo
 - Ao lado do IP
 - Mais eficiente
 - É mais fácil assegurar segurança fluxo-a-fluxo



(c) Sílvia Farraposo, Miguel Frade

10



Localização (3)

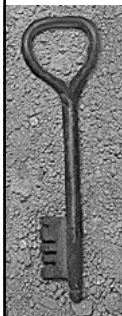
Camada de Aplicação
Transporte
Rede
IPSec
Ligação Dados

♦ *Bump In The Stack* (BITS)

- Não são necessárias alterações à pilha protocolar
- Implica a duplicação de algumas funções IP
- Menos eficiente e versátil

(c) Sílvia Farraposo, Miguel Frade

11



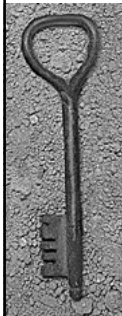
Localização (4)

♦ Nos routers

- Segurança entre LANs sobre a Internet
- Transparente para os utilizadores finais
- Facilita a autenticação de utilizadores à entrada das redes privadas
- Funciona associado ao NAT e a IPs privados
- Duas alternativas
 - Em modo nativo
 - Bump In The Wire (BITW)

(c) Sílvia Farraposo, Miguel Frade

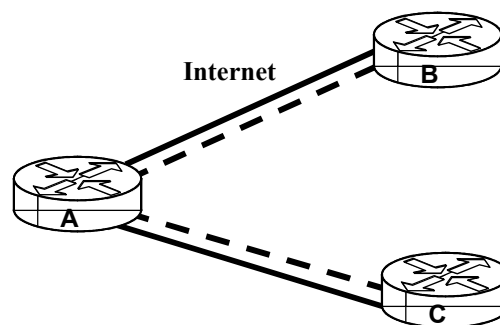
12



Localização (5)

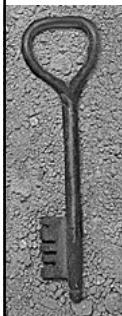
♦ Modo nativo

- IPSec integrado na pilha protocolar do router



(c) Sílvia Farraposo, Miguel Frade

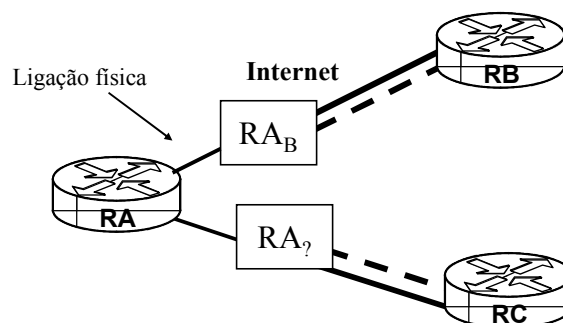
13



Localização (6)

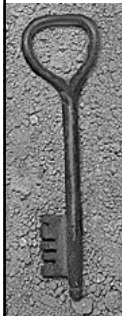
♦ Bump In The Wire (BITW)

- Utilização de hardware adicional entre o router e a linha



(c) Sílvia Farraposo, Miguel Frade

14

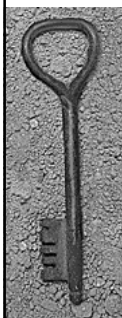


Associações de Segurança (1)

- ◆ Security Association (SA)
 - Espécie de contracto entre o emissor e o receptor
 - Definem todos os elementos necessários para se proceder à comunicação de forma segura
 - É unidireccional (para uma comunicação de dados bidireccional são necessários dois SA's).
 - São identificados de forma unívoca por três parâmetros:
 - o SPI (*Security Parameters Index*), que é um número de identificação local do SA
 - o endereço IP de destino
 - o *Security Protocol Identifier* que indica se o protocolo a usar no SA é o AH ou o ESP.
 - Todos os SA's são guardados numa base de dados denominada SAD (*Security Association Database*)

(c) Sílvia Farraposo, Miguel Frade

15

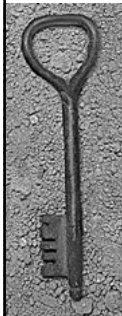


Associações de Segurança (2)

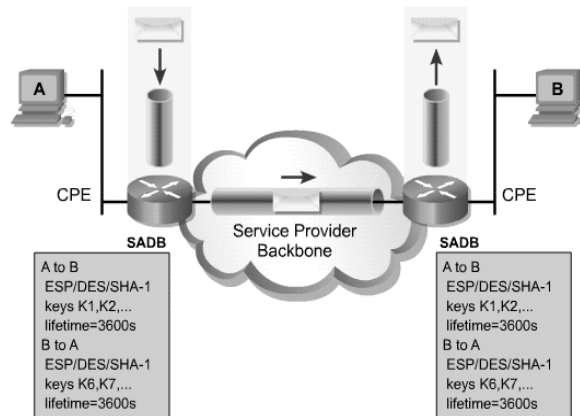
- ◆ Parâmetros guardados na SAD:
 - Contador de número de sequência
 - Sequence Counter Overflow
 - Anty-replay Window
 - Informação AH (algoritmos, chaves, validade, ...)
 - Informação ESP (chaves, valores de inicialização, algoritmos, ...)
 - Tempo de vida da SA
 - Modo IPsec (transporte ou túnel)
 - Path MTU (tamanho máximo sem fragmentação)

(c) Sílvia Farraposo, Miguel Frade

16

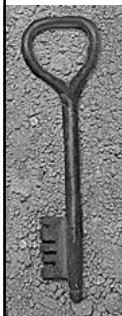


Associações de Segurança (3)



(c) Sílvia Farraposo, Miguel Frade

17

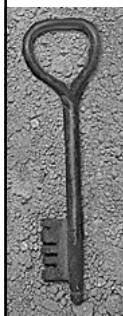


Associações de Segurança (4)

- ◆ A discriminação do tráfego a proteger é feita na SPD (security policy database), baseada em selectores:
 - Endereço IP origem e destino
 - UserID (válido se o IPSec estiver no mesmo SO do utilizador)
 - Nível de segurança
 - Protocolo da camada de transporte
 - Protocolo IPSec (AH e/ou ESP)
 - Portos origem e destino
 - Tipo de serviço

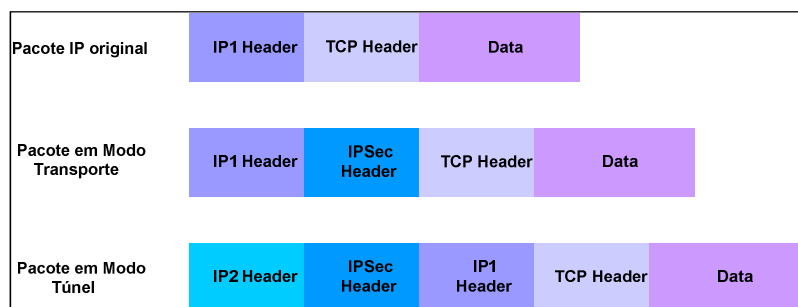
(c) Sílvia Farraposo, Miguel Frade

18



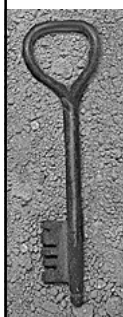
Modos de Operação (1)

- ◆ Transporte
- ◆ Túnel



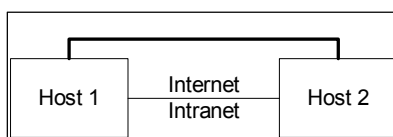
(c) Sílvia Farraposo, Miguel Frade

19



Modos de Operação (2)

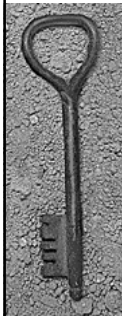
- ◆ Ponto a ponto



Transporte	Túnel
[IP1][AH][upper]	[IP2][AH][IP1][upper]
[IP1][ESP][upper]	[IP2][ESP][IP1][upper]
[IP1][AH][ESP][upper]	

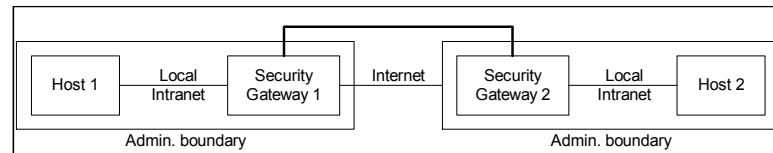
(c) Sílvia Farraposo, Miguel Frade

20



Modos de Operação (3)

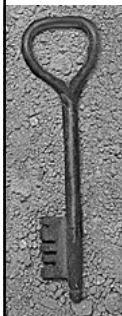
◆ VPN



Transporte	Túnel
(não pode ser usado)	[IP2][AH][IP1][upper]
	[IP2][ESP][IP1][upper]

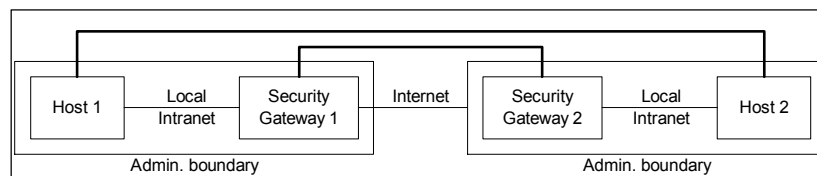
(c) Sílvia Farraposo, Miguel Frade

21



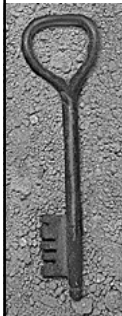
Modos de Operação (4)

◆ Combinação do modo VPN com o modo ponto a ponto



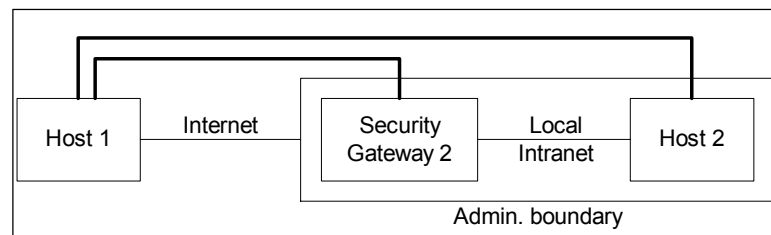
(c) Sílvia Farraposo, Miguel Frade

22



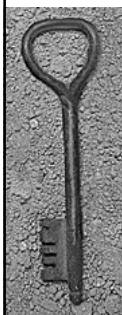
Modos de Operação (5)

◆ Ligação remota via Internet



(c) Sílvia Farraposo, Miguel Frade

23

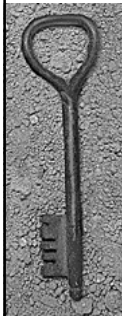


Authentication Header (1)

- ◆ Definido no RFC 4302
- ◆ Garante a integridade e autenticação dos pacotes IP (dos campos imutáveis e dos mutáveis, mas previsíveis)
- ◆ Não permite a cifragem de pacotes IP
- ◆ Pode ser aplicado sozinho ou em combinação com o ESP
- ◆ Permite o uso de algoritmos existentes
 - HMAC-MD5 (por omissão)
 - HMAC-SHA-1

(c) Sílvia Farraposo, Miguel Frade

24



Authentication Header (2)

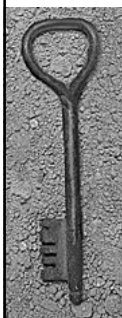
◆ Formato do cabeçalho

- SPI - Security Parameters Index
- Número de sequência
- Parâmetros e dados para autenticação

Next Header	Payload Len	RESERVED
Security Parameters Index (SPI)		
Sequence Number Field		
Authentication Data (variable)		

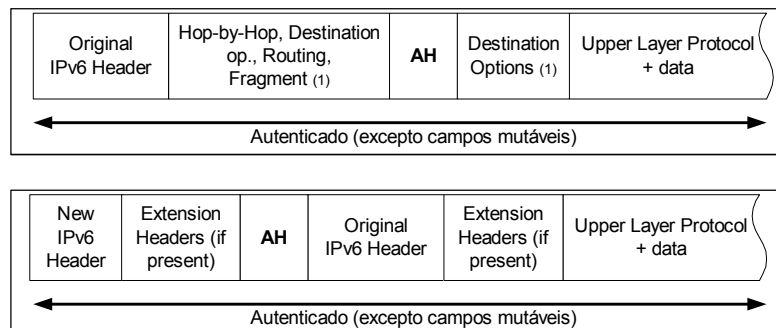
(c) Sílvia Farraposo, Miguel Frade

25



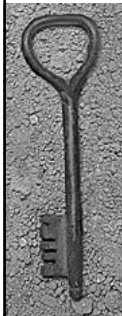
Authentication Header (3)

- ### ◆ A cobertura da autenticação AH é superior à cobertura de autenticação do ESP



(c) Sílvia Farraposo, Miguel Frade

26

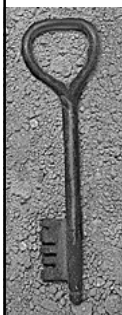


Encapsulating Security Payload (1)

- ◆ Definido no RFC 4303
- ◆ Garante a integridade dos pacotes IP
- ◆ Permite a cifragem de pacotes IP
- ◆ Suporte de diversos algoritmos:
 - DES (no modo Cypher Block Chaining): por omissão
 - 3-DES
 - MD5 (por omissão) e SHA-1 para autenticação
 - Sem autenticação, ou sem confidencialidade

(c) Sílvia Farraposo, Miguel Frade

27



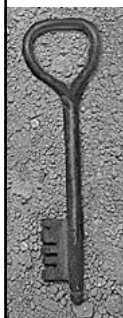
Encapsulating Security Payload (2)

- ◆ Formato do cabeçalho
 - SPI - Security Parameters Index
 - Número de sequência
 - Parâmetros e dados para cifragem
 - Parâmetros e dados para autenticação

Security Parameters Index (SPI)		
Sequence Number Field		
Payload Data (variable)		
Padding (0 - 255 Bytes)		
	Pad Length	Next Header
Authentication Data (variable)		

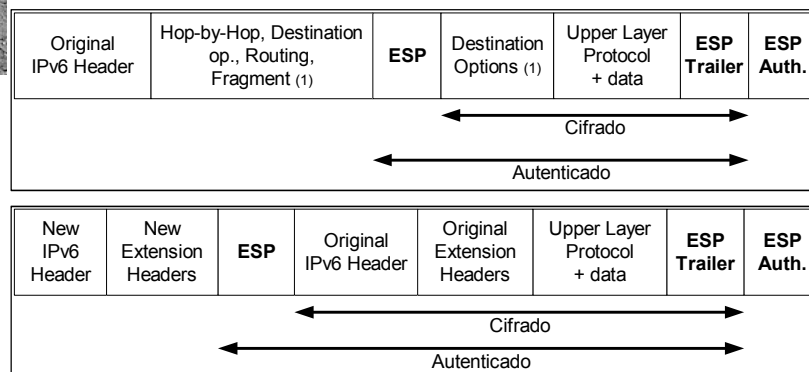
(c) Sílvia Farraposo, Miguel Frade

28



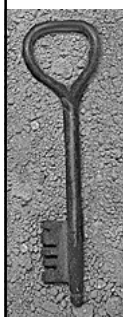
Encapsulating Security Payload (3)

- ◆ ESP no modo de transporte e túnel



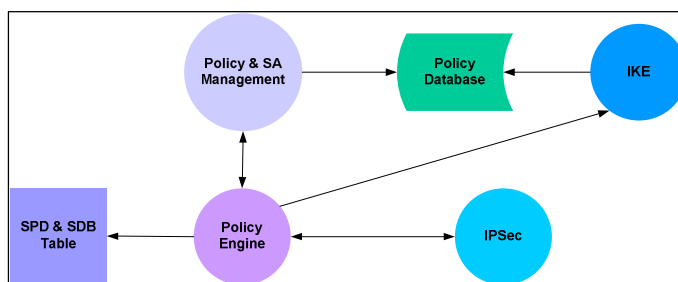
(c) Sílvia Farraposo, Miguel Frade

29



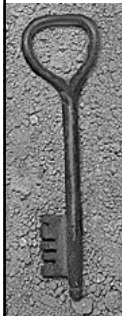
Implementação do IPSec (1)

- ◆ Protocolos IPSec
- ◆ Security Policy Database (SPD)
- ◆ Security Association Database (SAD)
- ◆ Internet KEY Exchange (IKE)
- ◆ Gestão e implementação da política



(c) Sílvia Farraposo, Miguel Frade

30



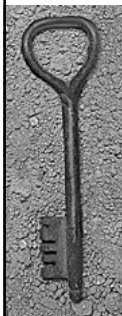
Implementação do IPSec (2)

IKE Policy Parameters

Parameter	Strong	Keyword	Default
Message encryption algorithm	DES 3-DES	des 3des	768-bit Diffie-Hellman
Message integrity has algorithm	SHA-1, HMAC variant MD5, HMAC variant	sha md5	86400 seconds, or one day
Peer authentication method	Pre-shared keys RSA encrypted nonces RSA signatures	pre-share rsa-encr rsa-sig	768-bit Diffie-Hellman
Key exchange parameters, Diffie-Hellman group identifier	768-bit Diffie-Hellman or 1024-bit Diffie-Hellman	1 2	768-bit Diffie-Hellman
ISAKMP-established security associations lifetime	Can specify any number of seconds	-	86400 seconds, or one day

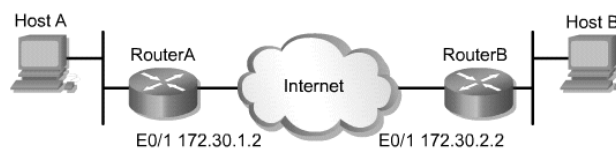
(c) Sílvia Farraposo, Miguel Frade

31



Implementação do IPSec (3)

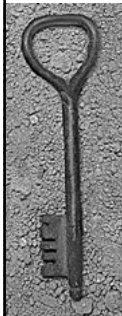
Exemplo de uma Política IPSec



Policy	Host A	Host B
Transform set	ESP-DES, Tunnel	ESP-DES, Tunnel
Peer hostname	RouterB	RouterA
Peer IP address	172.30.2.2	172.30.1.2
Hosts to be encrypted	10.0.1.3	10.0.2.3
Traffic (packet) type to be encrypted	TCP	TCP
SA establishment	ipsec-isakmp	ipsec-isakmp

(c) Sílvia Farraposo, Miguel Frade

32

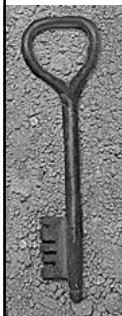


Gestão de Chaves (1)

- ♦ Manual
 - Utilizada na fase inicial da implementação
 - Introdução manual das chaves nos extremos das ligações IPSec
- ♦ Automática:
 - IKE (*Internet Key Exchange*)
 - RFC 2409
 - Usado para definir Associações de Segurança (SAs) entre entidades
 - Baseado no ISAKM (Internet Security Association and Key Management Protocol)/Oakley do IETF
 - Troca de parâmetros de segurança SPD (*Security Parameters Definition*)
 - Troca de chaves públicas (Diffie-Hellman)
 - Para além do IPSec pode ser utilizado noutros domínios dependendo do DOI (Domain of Interpretation)
 - Outros
 - SNKI (Sun)
 - Photuris

(c) Sílvia Farraposo, Miguel Frade

33

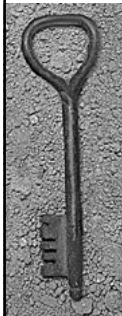


Gestão de Chaves (2)

- ♦ ISAKMP/Oakley
 - Oakley Key Determination Protocol
 - Protocolo baseado no algoritmo Diffie-Hellman, mas mais seguro
 - Protocolo genérico que não especifica formatos
 - Internet Security Association and Key Management Protocol
 - Estrutura para a gestão de chaves na Internet
 - Especifica formatos

(c) Sílvia Farraposo, Miguel Frade

34



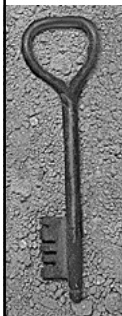
Gestão de Chaves (3)

♦ Oakley Key Determination Protocol

- Cada estação envolvida tem uma chave privada e uma pública
- A chave secreta da sessão é calculada com base na chave privada e na chave pública da estação remota
- Utilização de um mecanismo de *cookies* para evitar os ataques por entupimento
- Prevenção de ataques de *replay* através de *nonces*
- Usa autenticação para prevenir ataques *man-in-the-middle*

(c) Sílvia Farraposo, Miguel Frade

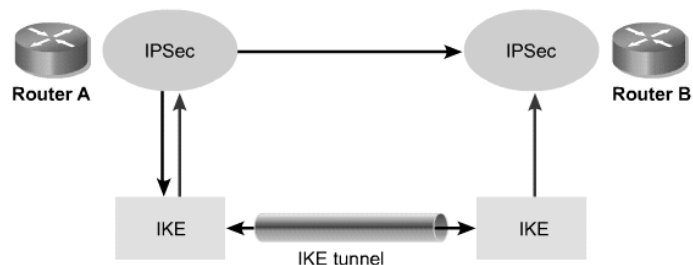
35



Gestão de Chaves (3)

1. Outbound packet is sent from RouterA to RouterB. No IPSec SA.

4. Packet is sent from RouterA to RouterB, protected by IPSec SA.

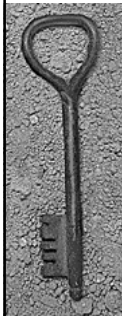


2. RouterA's IKE begins negotiation with RouterB's IKE.

3. Negotiation complete. RouterA and RouterB now have a complete set of SAs in place.

(c) Sílvia Farraposo, Miguel Frade

36



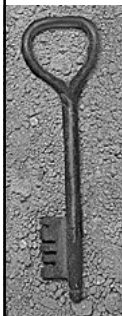
Gestão de Chaves (4)

IKE Policy Parameters

Parameter	Strong	Keyword	Default
Message encryption algorithm	DES 3-DES	des 3des	768-bit Diffie-Hellman
Message integrity has algorithm	SHA-1, HMAC variant MD5, HMAC variant	sha md5	86400 seconds, or one day
Peer authentication method	Pre-shared keys RSA encrypted nonces RSA signatures	pre-share rsa-encr rsa-sig	768-bit Diffie-Hellman
Key exchange parameters, Diffie-Hellman group identifier	768-bit Diffie-Hellman or 1024-bit Diffie-Hellman	1 2	768-bit Diffie-Hellman
ISAKMP-established security associations lifetime	Can specify any number of seconds	-	86400 seconds, or one day

(c) Sílvia Farraposo, Miguel Frade

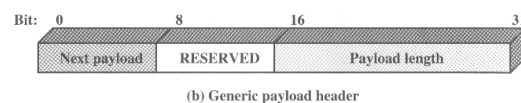
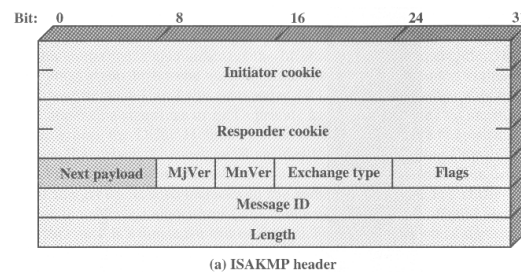
37



Gestão de Chaves (5)

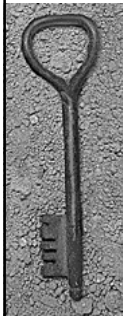
♦ ISAKMP

- Mensagens trocadas sobre UDP



(c) Sílvia Farraposo, Miguel Frade

38



Gestão de Chaves (6)

♦ Trocas ISAKMP

- *Base Exchange*
 - Troca de chaves e autenticação transmitidas juntas
 - Minimiza as trocas (4 mensagens)
 - Mas não fornece protecção de identidade
- *Identity Protection Exchange*
 - Extensão do *Base Exchange* para dar protecção de identidade (6 mensagens)
- *Authentication Only Exchange*
 - Efectua autenticação mútua sem troca de chaves (3 mensagens)
- *Aggressive Exchange*
 - Minimiza a troca de mensagens (3 mensagens)
- *Informational Exchange*
 - Usado para transportar informação de gestão de SA's