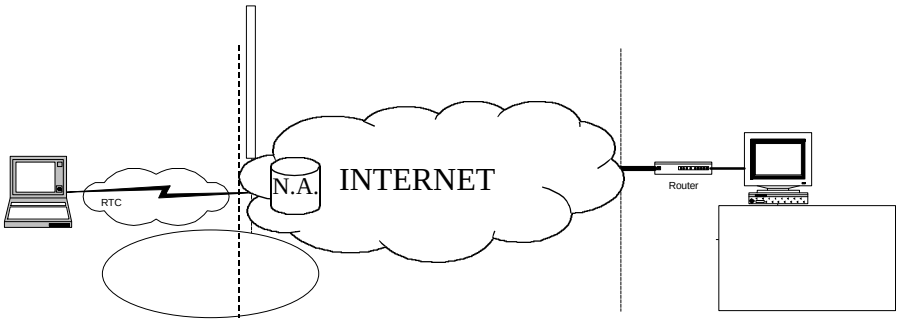
Seguridad en Internet
VPN–IPSEC

Olga Sánchez Campoy
osanchez@mat.upc.es

Contenido

- Entorno real. VPN – IPSEC
- Aspectos técnicos. VPNs
  - PPTP (Point–to–Point Tunneling Protocol)
  - L2F (Layer 2 Forwarding)
  - L2TP (Layer 2 Tunneling Protocol)
  - IPSEC
- Productos certificados IPSEC (ICSA)
- Referencias

Redes Privadas Virtuales



Aspectos técnicos VPNs

- Nivel 2
  - PPTP, L2F, L2TP
- Nivel 3
  - IPSEC

Nivel 2

Point–to–Point Tunneling Protocol

- Creado por Microsoft, 3COM y ECI Telematics Internacional (arquitectura original Ascend)

Layer 2 Forwarding

- Creado por Cisco (con apoyo de Nortel y Shiva)

Tunneling multiprotocolo
LAN a LAN y Acceso Remoto a LAN
No ofrece seguridad de datos

Nivel 2: L2TP

Layer 2 Tunneling Protocol

- Recoge las características de PPTP y L2F
- Tunneling a nivel de enlace de PPP
- LAN a LAN y Acceso Remoto a LAN
- No da seguridad a los datos –> IPSEC
- Multifabricante

IPSEC (RFC 2401)

- IPSEC proporciona servicios de seguridad a Nivel 3.
- Permite seleccionar protocolo de seguridad, algoritmos que se van a utilizar y las claves requeridas para dar esto servicios.
- Servicios de seguridad: control de acceso, integridad, autenticación del origen de los datos, confidencialidad.

Servicios IPSEC

- Protocolos de seguridad
  - AH (Authentication Header): Integridad y autenticación de origen (HMAC, MD5, SHA–1)
  - ESP (Encapsulating Security Payload): Confidencialidad (DES, 3DES, RC5, IDEA)
  - AH y ESP proporcionan control de acceso. Pueden ser aplicados solos o en combinación para proporcionar la seguridad deseada
- Gestión de claves
  - IKE (Internet Key Exchange): Establece la comunicación segura (Security Association y clave DH)

Protocolos de seguridad: AH y ESP

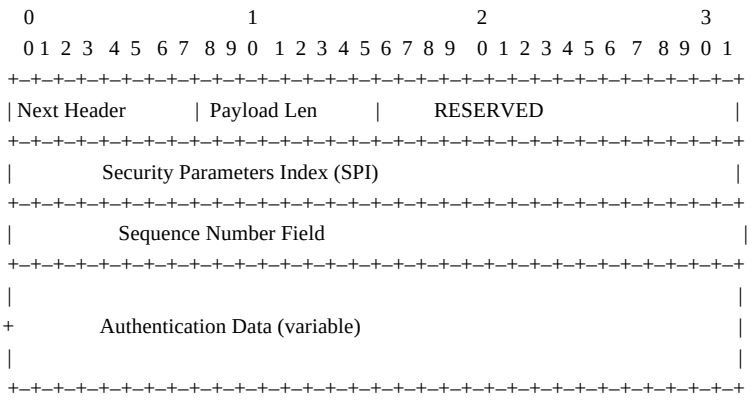
Modos de funcionamiento:

- Modo transporte
  - Entre hosts
  - La cabecera del protocolo aparece después de la cabecera IP y antes
- Modo túnel
  - Entre hosts y gateways
  - Existe una cabecera IP se salida y otra de entrada

AH (RFC 2402)

- Integridad y autenticación de origen
- Está insertado entre la cabecera IP y los datos del paquete IP
- Puede aplicarse solo o junto ESP

Formato AH



Formato AH

- Next Header.
  - Identifica el tipo de los siguientes datos después de la cabecera de autenticación
- Payload Length
  - Especifica la longitud de AH
- Reserved
  - Uso futuro
- SPI
  - En combinación con la IP de destino y protocolo de seguridad, únicamente identifica el SA para este datagrama

Formato AH

- Secuence Number
  - Contador incremental
- Authentication data
  - Es de tamaño variable. Contiene el ICV (Integrity Check Value)
  - El algoritmo de autenticación que utiliza MACs (Message Authentication Codes) MD5 o SHA-1

Modos de funcionamiento AH

- Modo transporte

Antes:

```
----------------------------
| IP origen | TCP | Datos |
----------------------------
```

Después:

```
-----------------------------------
| IP origen | AH | TCP | Datos |
-----------------------------------
```

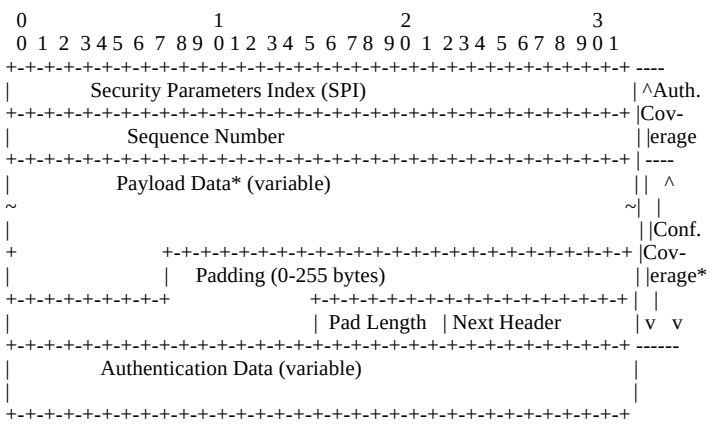
Modos de funcionamiento AH

- Modo túnel

ESP (RFC 2406)

- Confidencialidad
- Puede aplicarse solo o junto AH
- Proporciona servicios de seguridad mixtos entre hosts y gateways
- Está insertado entre la cabecera IP y los datos del paquete IP cifrado

Formato ESP



Formato ESP

- SPI
  - En combinación con la IP de destino y protocolo de seguridad, únicamente identifica el SA para este datagrama
- Secuence Number
  - Contador incremental
- Payload Data
  - Es de longitud variable contiene los datos descritos por el campo Next Header

Formato ESP

- Padding
  - Relleno
- Pad Length
  - Longitud de los bytes que le preceden
- Next Header
  - Identifica el tipo de dato contenido en el campo de datos útiles
- Authentication Data
  - Es de tamaño variable. Contiene el ICV (Integrity Check Value)

Modos de funcionamiento: ESP

- Modo transporte

| orig IP hdr | ESP hdr | *TCP* | *Data* | *ESP Trailer* | ESP Auth |

- Modo túnel

| new orig IP hdr | ESP hdr | *orig IP hdr* | *TCP* | *Data* | *ESP Trailer* | ESP Auth |

IKE (RFC 2409)

Gestión de claves

- Manual Key Exchange ⇒ Entornos pequeños
- Simple Key Interchange Protocol (SKIP) ⇒ Sun Microsystems
- Internet Security Association & Key Management Protocol (ISAKMP)
- Oakley Key Exchange Protocol

IKE

ISAKMP

- Proporciona un marco de operación para la gestión de claves de Internet y el soporte de protocolo específico para negociar los atributos de seguridad
- NO establece las claves de sesión

Oakley

- Diffie–Helman para establecer las claves de sesión en los routers o hosts
- Puede utilizarse solo o con el ISAKMP si necesita negociación de atributos

ISAKMP con Oakley

Estructura de ISAKMP junto con los modos de intercambio de claves de Oakley (DH)

IKE

- Fase1: Los nodos IPSEC establecen un canal seguro para realizar el intercambio de información (SA)
  - Modo principal. Protección identidad
  - Modo agresivo
- Fase 2: Los nodos IPSEC negocian por el canal establecido
  - Modo rápido

Modo grupo nuevo -> Futuras negociaciones

IKE

Atributos de seguridad que se negocian en el SA:

- Algoritmo de cifrado
- Algoritmo hash
- Método de autenticación
- Información sobre el grupo Diffie-Hellman

Main Mode

- Los 2 primeros mensajes negocian la seguridad.
- Los dos siguientes los valores públicos para el intercabio DH
- Los dos últimos autentifican el intercambio DH

Agressive Mode

- Los 2 primeros mensajes negocian la política, los valores públicos para hacer el intercambio DH y las identidades
- El segundo mensaje sirve para autenticar al receptor
- El tercer mensaje autentica al iniciador y proporciona una prueba de la participación en el intercambio
- Limitación respecto a Main Mode

Fase1: Autenticación con firmas

Main Mode

Initiator		Responder
HDR, SA	⇒	
	⇐	HDR, SA
HDR, KE, Ni	⇒	
	⇐	HDR, KE, Nr
HDR*, IDii, [CERT,] SIG_I	⇒	
	⇐	HDR*, IDir, [CERT,] SIG_R

Fase1: Autenticación con firmas

Agresive Mode

Initiator		Responder
HDR, SA, KE, Ni, IDii	⇒	
	⇐	HDR, SA, KE, Nr, IDir, [CERT,] SIG_R
HDR, [CERT,] SIG_I	⇒	

Fase1: Autenticación con cifrado de clave pública

Main mode

Initiator		Responder
HDR, SA	⇒	
	⇐	HDR, SA
HDR, KE, [HASH(1),] <IDii_b>PubKey_r, <Ni_b>PubKey_r	⇒	
		HDR, KE, <IDir_b>PubKey_i,
	⇐	<Nr_b>PubKey_i
HDR*, HASH_I	⇒	
	⇐	HDR*, HASH_R

Fase1: Autenticación con cifrado de clave pública

Agresive Mode

Initiator		Responder
HDR, SA, [HASH(1),] KE, <IDii_b>Pubkey_r, <Ni_b>Pubkey_r	⇒	
		HDR, SA, KE, <IDir_b>PubKey_i,
	⇐	<Nr_b>PubKey_i, HASH_R
HDR, HASH_I	⇒	

Fase1: Autenticación con un modo revisado de cifrado de clave pública

Main Mode

Initiator		Responder
HDR, SA	⇒	
	⇐	HDR, SA
HDR, [HASH(1),] <Ni_b>Pubkey_r, <KE_b>Ke_i, <IDii_b>Ke_i, [<<Cert-I_b>Ke_i]	⇒	
	⇐	HDR, <Nr_b>PubKey_i, <KE_b>Ke_r,<IDir_b>Ke_r,
HDR*, HASH_I	⇒	
	⇐	HDR*, HASH_R

Fase1: Autenticación con un modo revisado de cifrado de clave pública

Aggressive Mode

Initiator		Responder
HDR, SA, [HASH(1),] <Ni_b>Pubkey_r,<KE_b>Ke_i, <IDii_b>Ke_i [, <Cert-I_b>Ke_i]	⇒	
		HDR, SA, <Nr_b>PubKey_i, <KE_b>Ke_r, <IDir_b>Ke_r,
	⇐	HASH_R
HDR, HASH_I	⇒	

Fase1: Autenticación clave precompartida

Main Mode

Initiator		Responder
HDR, SA	⇒	
	⇐	HDR, SA
HDR, KE, Ni	⇒	
	⇐	HDR, KE, Nr
HDR*, IDii, HASH_I	⇒	
	⇐	HDR*, IDir, HASH_R

Fase1: Autenticación clave precompartida

Aggressive mode

Initiator		Responder
HDR, SA, KE, Ni, IDii	⇒	
	⇐	HDR, SA, KE, Nr, IDir, HASH_R
HDR, HASH_I	⇒	

Fase 2: Quick Mode

Initiator		Responder
HDR*, HASH(1), SA, Ni [, KE] [, IDci, IDcr]	⇒	
	⇐	HDR*, HASH(2), SA, Nr [, KE] [, IDci, IDcr]
HDR*, HASH(3)	⇒	

New Group Mode

Initiator		Responder
HDR*, HASH(1), SA	⇒	
	⇐	HDR*, HASH(2), SA

Productos certificados IPSEC (International Computer Security Association)

Programas de certificación

- Versión 1.0 (requisitos básicos de autenticación, integridad y confidencialidad)
- Versión 1.0A (incluye SHA1, ESP NULL)
- Strong Cryto (Scr) (incluye 3DES, DH grupo 2, opcional CAST, IDEA, RC5)
- Enhanced Funcionality (idem v 1.0A más compresión)
- Versión 1.1 (idem v 1.0A más certificados)
- Enhanced Certificate Authority (idem Versión 1.1 más procesamiento automatizado de certificados)

IPSEC v1.0 POR LA ICSA

EMPRESA	PRODUCTO	PLATAFORMA
Axent Technologies	Raptor Firewall's VPN Server v6.0	Windows NT
Chek Point Software	Firewall-1 v4.0 (b4.01.3)	NT Solaris
Network Associates	Gaunlet VPN v5.0	NT, Solaris, HP-UX
Cisco Systems	Cisco IOS v11.3.3	IOS
IBM Corporation	OS/400 V4R4 VPN	As 400
RadGuard	ClPro VPN Hardware v1.12 Software v 3.22 vb3	Hardware Propietario

Datos facilitados por SIC Febrero 2000

Referencias

IPSEC Working Group page

http://www.ietf.org/html.charters/ipsec–charter.html

Preguntas

Olga Sánchez Campoy