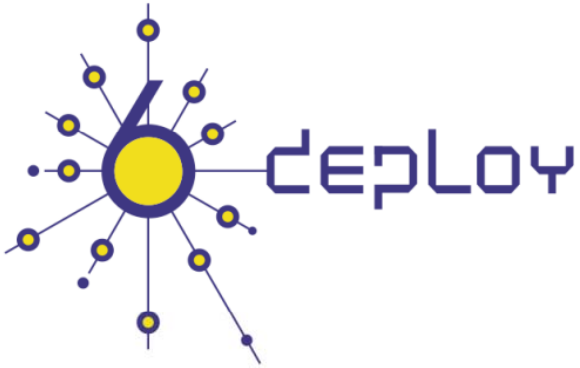
Curso IPv6

WALC 2009

Bogotá – Colombia

21 al 25 Septiembre 2009



César Olvera (cesar.olvera@consulintel.es)

Alvaro Vives (alvaro.vives@consulintel.es)

deploy

Consulintel

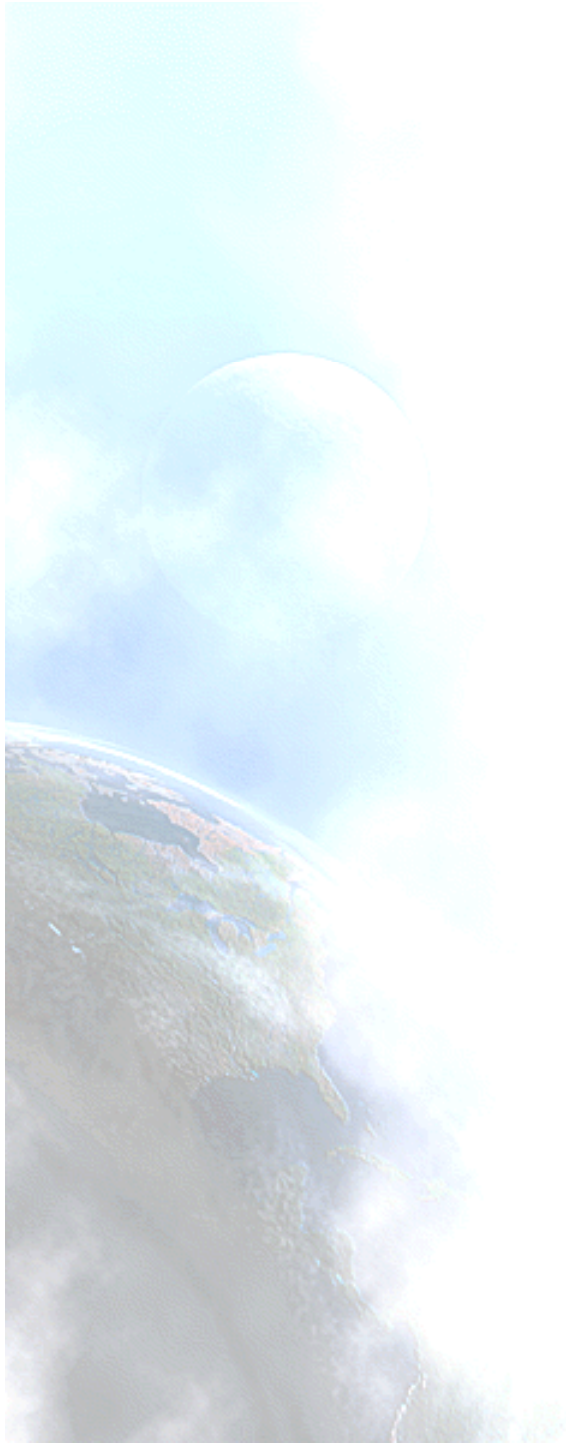
Consultores Integrales en Telecomunicaciones

Contenido del curso (1)

- **Bloque 1. Tutorial IPv6**
  1. Introducción a IPv6
  2. Formatos de cabeceras y tamaño de paquetes
  3. Direccionamiento IPv6
  4. ICMPv6, Neighbor Discovery y DHCPv6
  5. Seguridad IPv6
  6. Encaminamiento con IPv6
  7. Mecanismos de Transición
  8. Movilidad IPv6

Contenido del curso (2)

- **Bloque 2. Otros Aspectos Avanzados**
  9. Calidad de Servicio (QoS)
  10. Multicast
  11. Multi-homing
  12. Porting de aplicaciones
  13. Gestión SNMP sobre IPv6
  14. IPv6 sobre MPLS
  15. DNS IPv6



Bloque 1

Tutorial IPv6

5. Seguridad IPv6

5.1 Introducción
5.2 IPsec: La teoría
5.3 Extensiones de Privacidad
5.4 Amenazas a ND
5.5 Comparativa IPv4 vs. IPv6
5.6 Aspectos de seguridad con IPv6
5.7 Temas prácticos
5.8 Firewalling
5.9 Modelo de Seguridad Distribuida

5.1 Introducción

Introducción

- Aunque el término Seguridad abarque gran cantidad de temas, en esta sección se abordarán solamente los relacionados con IPv6
- En primer lugar se dará una descripción de IPsec debido a que es obligatoria su implementación en todas las pilas IPv6, proporcionando la posibilidad de su uso a todos los dispositivos IPv6.
- A continuación se tratarán algunas soluciones de seguridad concretas desarrolladas en el contexto de IPv6: Extensiones de Privacidad y SEND.
- Se compararán IPv6 e IPv4 desde el punto de vista de las amenazas a la seguridad.
- Se expondrá un análisis general desde el punto de vista práctico, comparando elementos de seguridad IPv4 e IPv6.
- Por último se introducirá el concepto de Seguridad Distribuida.

5.2 IPsec: La teoría

Seguridad IP (IPsec)

- **Objetivos**:
  - Proporcionar seguridad criptográfica, de calidad e interoperable para IPv4 e IPv6.
  - No afectar negativamente a usuarios, hosts u otros componentes de Internet que no usen IPsec para la protección del tráfico.
  - Los protocolos de seguridad (AH, ESP e IKE) se han diseñado para ser independientes de los algoritmos de cifrado usados. Se define un conjunto de algoritmos por defecto.
- **Conjunto de Servicios de Seguridad**:
  - Control de Acceso
  - Integridad sin-conexión
  - Autentificación del origen de los datos
  - Protección contra reactuación (un tipo de integridad de secuencia parcial)
  - Confidencialidad (cifrado)
  - Confidencialidad de flujo de tráfico limitado

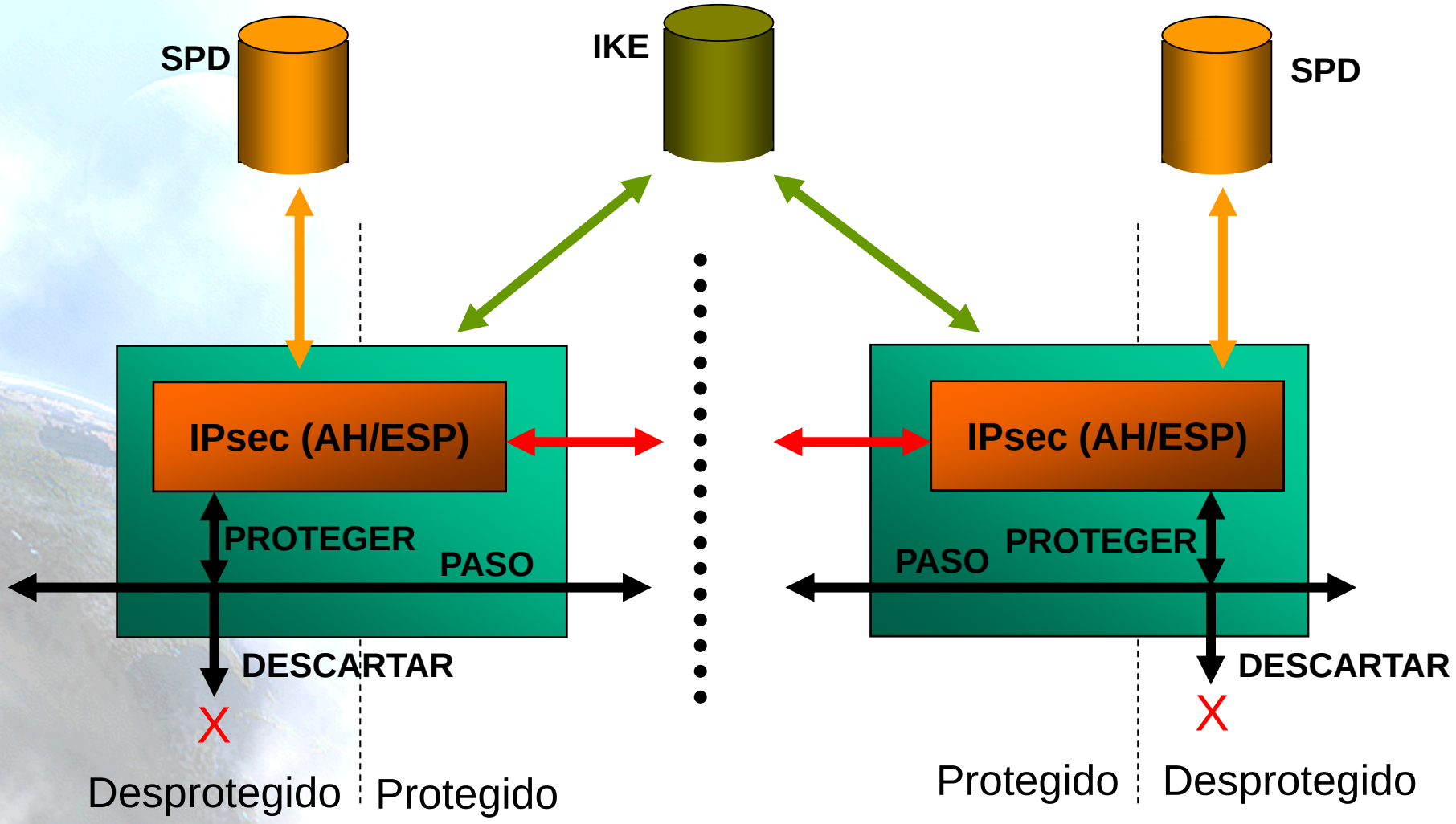
IPsec: Elementos Básicos

- Elementos básicos:
  - **Arquitectura Base** para sistemas conformes con IPsec (RFC4301)
  - **Protocolos de Seguridad:** Authentication Header (AH) (RFC4302) y Encapsulating Security Payload (ESP) (RFC4303)
  - **Asociaciones de Seguridad:** Qué son y como funcionan, cómo se gestionan (RFC4301)
  - **Gestión de Claves**: Manual y Automática (La Internet Key Exchange IKE) (RFC4306)
  - **Algoritmos para autentificación y cifrado**: Se definen algoritmos obligatorios, por defecto, para su uso con AH y ESP (RFC4835) y para IKEv2 (RFC4307)

Visión General (1)

- Una implementación IPsec opera en un host, como una pasarela de seguridad (SG) o como un dispositivo independiente.
- La protección ofrecida por IPsec se basa en los requerimientos definidos en la Security Policy Database (SPD).
- Los paquetes se clasifican basándose en información de las cabeceras IP y 'next layer', para buscar coincidencias en la SPD.
- Cada paquete puede ser DESCARTADO, PROTEGIDO usando los servicios IPsec o permitirse su PASO a través de la protección IPsec.
- IPsec se puede usar para proteger uno o más "caminos":
  - Entre un par de hosts.
  - Entre un par de pasarelas de seguridad.
  - Entre una pasarela de seguridad y un host.

Visión General (2)



PAD (Peer Authorization Database)

- La PAD proporciona un enlace entre la SPD y un protocolo de gestión de asociaciones de seguridad como IKE. Se encarga de varias funciones críticas:
  - Identificar peers o grupos de peers que están autorizados a comunicarse con la entidad IPsec.
  - Especifica el protocolo y el método usado para autentificar cada peer.
  - Proporciona los datos de autentificación para cada peer.
  - Limita los tipos y valores de IDs que puede usar un peer para crear una SA 'hijo', asegurando así que no use identidades, que se busquen en la SPD, que no esta autorizado a usar cuando se crea una SA hijo.
  - Información de localización de pasarela de un peer, e.g., dirección(es) IP o nombres DNS, PUEDEN incluirse para peers que se sabe están "detrás" de una pasarela de seguridad.

Protocolos de Seguridad

- Las implementaciones IPsec DEBEN soportar ESP y PUEDEN soportar AH. AH y ESP pueden aplicarse solas o en combinación con la otra.
- **AH** proporciona:
  - Integridad.
  - Autentificación del origen de los datos.
  - Opcionalmente (según criterio del receptor) servicio anti-reactuación.
- **ESP** proporciona:
  - Integridad.
  - Autentificación del origen de los datos.
  - Opcionalmente (según criterio del receptor) servicio anti-reactuación.
  - Confidencialidad (NO recomendada sin integridad).
- Ambas ofrecen control de acceso, impuesta a través de la distribución de claves criptográficas y la gestión de flujos de tráfico según dicte la SPD.
- Estos mecanismos están diseñados para ser independientes de los algoritmos.

SA: El Concepto

- La Asociación de Seguridad (Security Association - SA) es un concepto fundamental para IPsec:
  - **Una “conexión” simple que proporciona servicios de seguridad al tráfico que transporta.**
- AH y ESP usan SAs, de forma que todas las implementaciones DEBEN soportar el concepto de Asociación de Seguridad.
- Una de las principales funciones de IKE es el establecimiento y mantenimiento de SAs.
- Para asegurar un comunicación bidireccional típica entre dos nodos con IPsec, se necesitan dos SAs (una para cada dirección). IKE crea pares de SAs.

Identificación de SA

- Cada SA se identifica unívocamente por la terna:
  - Índice de Parámetros de Seguridad (Security Parameter Index - SPI)
    - Cadena de bits asignada a la SA (significado local), como puntero a una base de datos de SAs (SPD o Security Policy Database).
  - Dirección IP Destino
  - Identificador de protocolo de seguridad (AH o ESP)
- La dirección destino puede ser:
  - Dirección Unicast
  - Dirección Broadcast
  - Dirección Grupo Multicast

SA Database (SAD)

- En cada implementación IPsec existe una base de datos de SAs (SAD, Security Association Database).
- Cada entrada define los parámetros asociados con una SA.
- Cada SA tiene una entrada en la SAD.
- La SPD tiene punteros a entradas en la SAD, cuando se tiene que usar IPsec (PROTEGER).

Campos de la SAD (1)

- **Security Parameter Index (SPI):** Un valor de 32 bits seleccionado por el extremo receptor de una SA para identificar unívocamente la SA.
- **Sequence Number Counter:** Un contador de 64 bits usado para generar el número de secuencia transmitido en las cabeceras AH y ESP (los números de secuencia de 64 bits se usan por defecto, pero lo de 32 bitstambién se soportan si se negocian previamente).
- **Sequence Counter Overflow:** Un flag que indica si el desbordamiento del contador de número de secuencia debe generar un evento auditable y evitar el envío de más paquetes por la SA, o si se permite el reinicio del contador.
- **Anti-Replay Window:** Un contador de 64 bits y un bit-map (o equivalente) usado para determinar si un paquete AH o ESP de entrada es un reenvío.
- **AH Information:** Algoritmos de autentificación, claves, tiempos de vida, etc.
- **ESP Information:** Algoritmos de autentificación y cifrado, claves, tiempos de vida, valores iniciales, etc.
- **IPsec Protocol Mode:** Túnel o Transporte.
- **SA Lifetime:** Intervalo de tiempo o bytes de una SA.

Campos de la SAD (2)

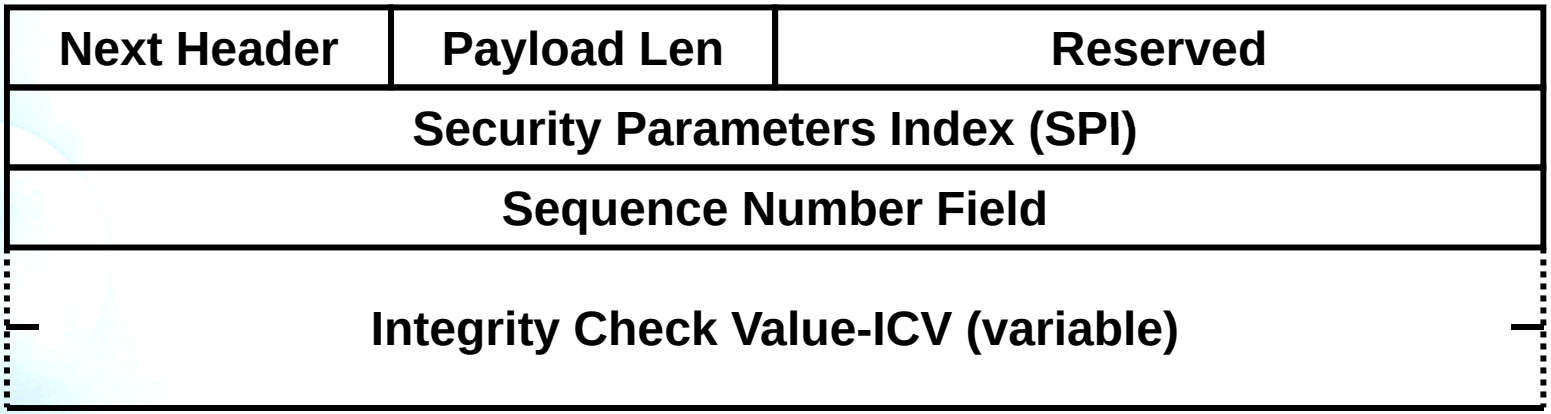
- **Stateful fragment checking flag**: Indica si se aplica o no comprobación de fragmentado a la SA.
- **DSCP values:** El conjunto de valores DSCP permitidos para los paquetes que van sobre esta SA. Si no se especifica ningún valor no se aplica ningún filtro DSCP.
- **Bypass DSCP (T/F)** o mapear a valores DSCP no protegidos si es necesario para restringir el paso de valores DSCP, aplicable a SAs en modo túnel.
- **Tunnel header IP source and destination address:** ambas direcciones deben ser o IPv4 o IPv6.
- **Path MTU:** Tamaño máximo de paquete transmitido sin fragmentar.

Transmisión IPsec

- Cabecera IPsec insertada entre la cabecera original y la carga.
- Si se usa ESP, los datos se cifran y se añade una 'coletilla' IPsec.

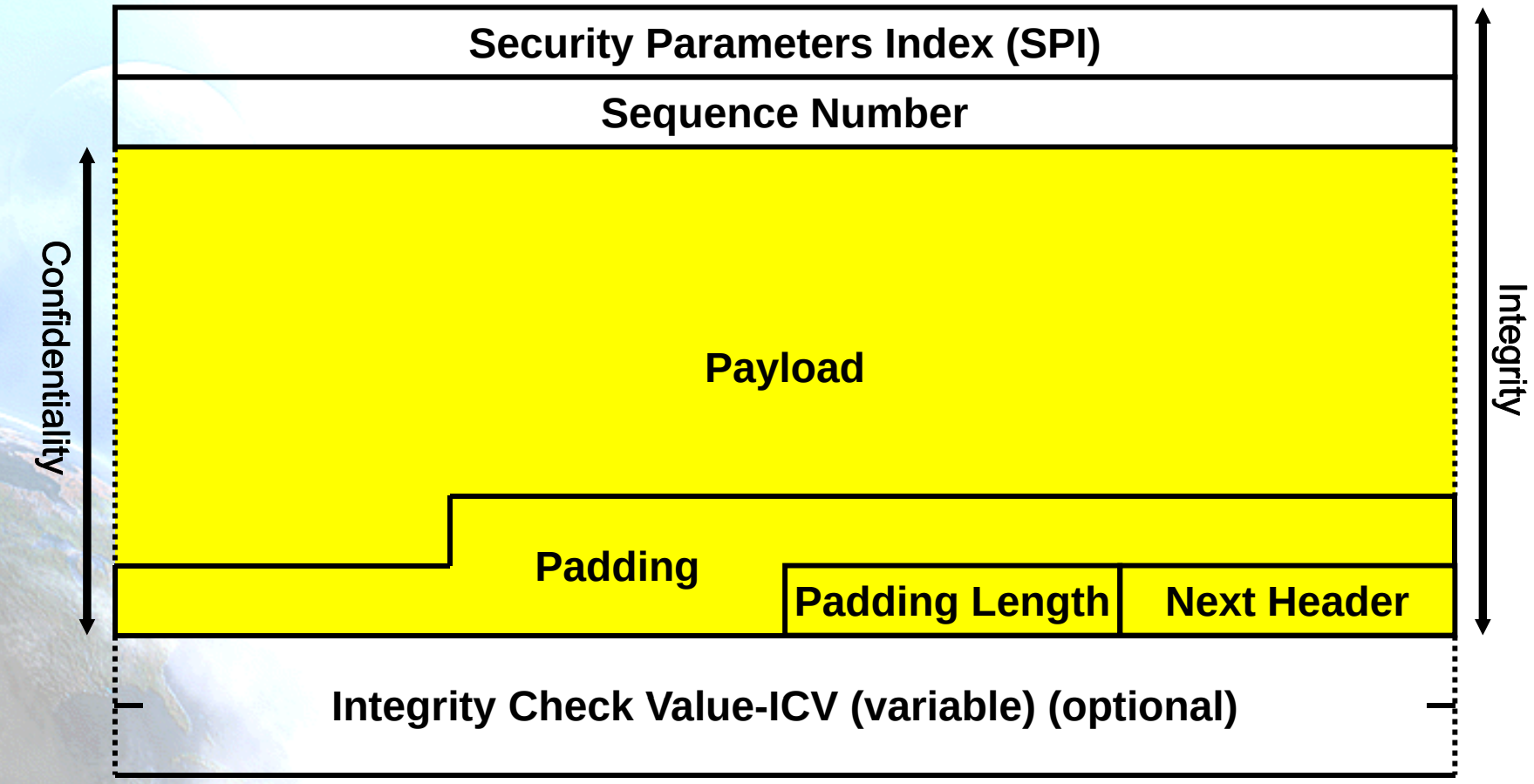
- Valor de Next Header:
  - ESP = 50
  - AH = 51

Cabecera AH (RFC4302)



- **SPI:** Valor arbitrario de 32 bits que usa el receptor para identificar la SA a la que pertenece un paquete que llega, el tipo de protocolo IPsec (AH) también puede ser necesario.
- **Sequence Number:** campo de 32 bits sin signo que contiene un contador que se incrementa en uno por cada paquete enviado, i.e., un número de secuencia de paquete para cada SA.
- **Integrity Check Value (ICV)**: Campo de longitud variable Variable. El campo debe tener un tamaño múltiplo de 32 bits (para IPv4 e IPv6).

Cabecera ESP (RFC4303)



Algoritmos ESP

- Especificados en la SA.
- Algoritmos de Cifrado ESP (RFC4835):
  - **MUST**: NULL (RFC2410), AES-CBC con clave de 128-bit (RFC3602)
  - **MUST-**: TripleDES-CBC (RFC2451)
  - **SHOULD**:AES-CTR (RFC3686)
  - **SHOULD NOT**: DES-CBC (RFC2405)
- Algoritmos de Autentificación ESP (RFC4835):
  - **MUST**: HMAC-SHA1-96 (RFC2404)
  - **SHOULD+**: AES-XCBC-MAC-96 (RFC3566)
  - **MAY**: NULL, HMAC-MD5-96 (RFC2403)

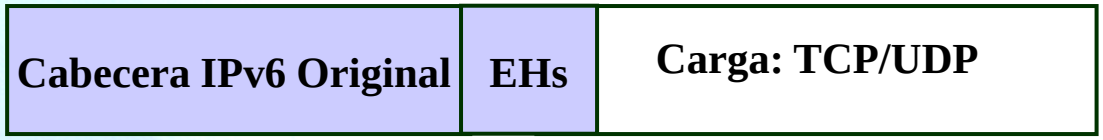
Algoritmos AH

- Especificados en la SA
- Algoritmos de Autentificación AH (RFC4835):
  - **MUST**: HMAC-SHA1-96 (RFC2404)
  - **SHOULD+**: AES-XCBC-MAC-96 (RFC3566)
  - **MAY**: HMAC-MD5-96 (RFC2403)

Modos de Uso

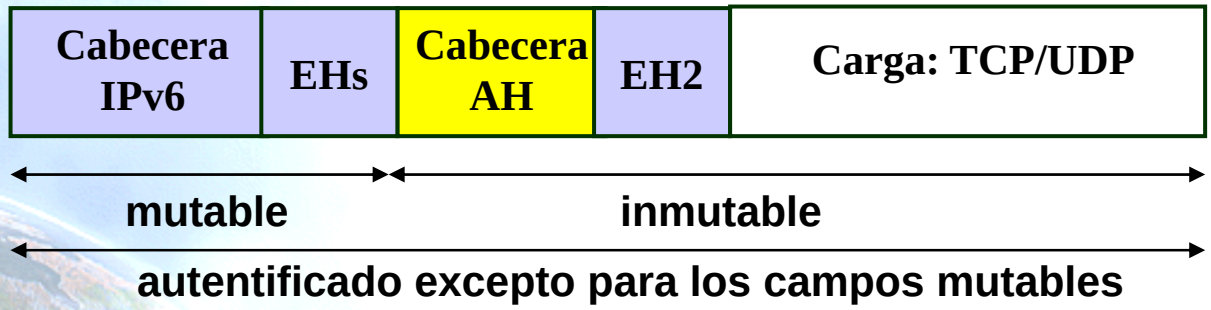
- Cada protocolo soporta dos modos de uso:
  - Modo Transporte (protege principalmente protocolos de capa superior)
    - Directo entre dos sistemas extremo-a-extremo
    - Los dos sistemas remotos deben soportar IPsec!
  - Modo Túnel (protocolos aplicados a paquetes IP encapsulados)
    - Túnel seguro para encapsular paquetes IP inseguros
    - Entre sistemas intermedios (no extremo-a-extremo)

AH en Modo Transporte y Túnel

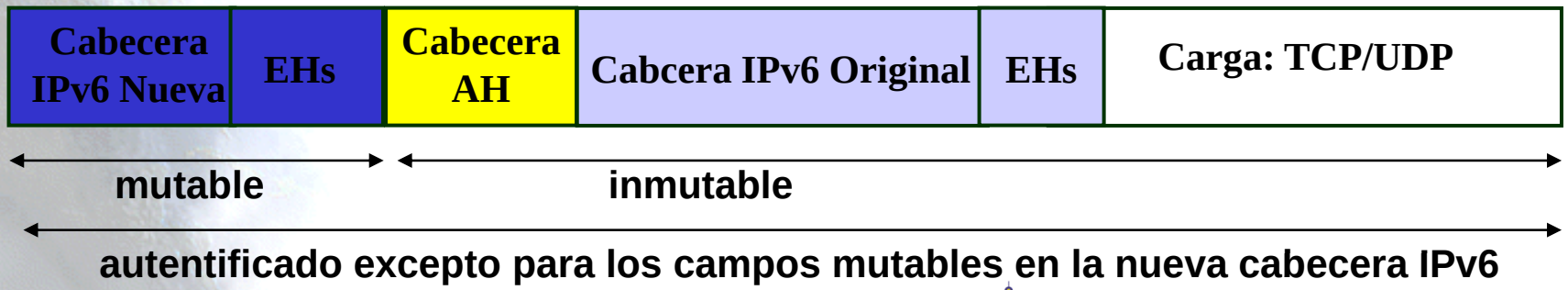


- EHs: Extension Headers: Hop-by-hop, Routing, Fragment, Dest. Option
- EH2: Destination Option Extension Header

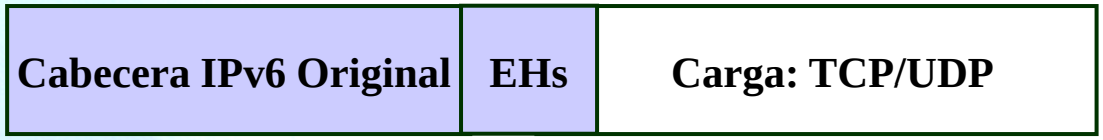
Modo Transporte



Modo Túnel

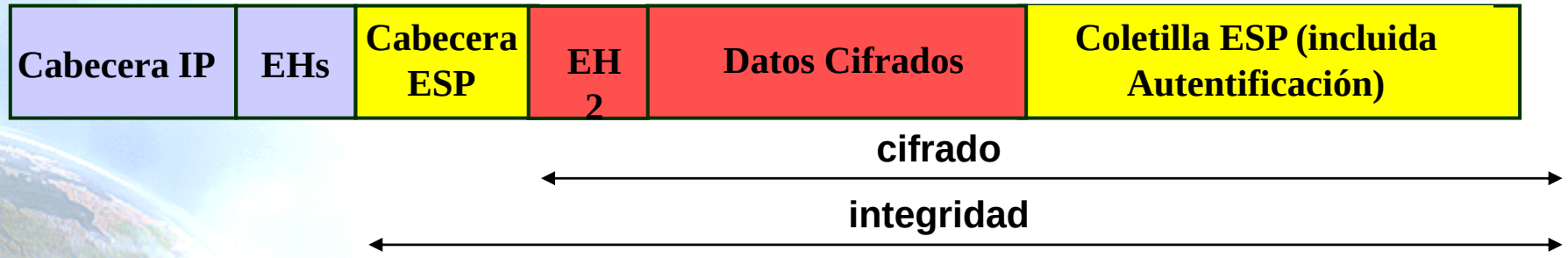


ESP en Modo Transporte y Túnel

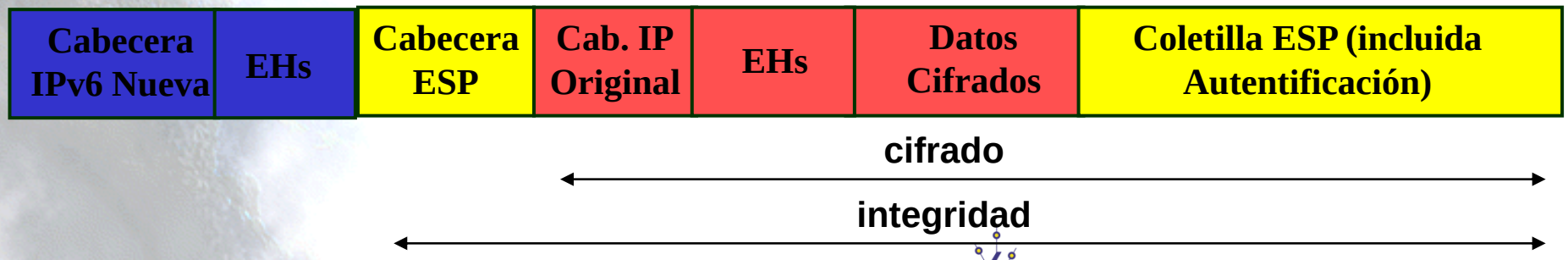


- EHs: Extension Headers: Hop-by-hop, Routing, Fragment, Dest. Option
- EH2: Destination Option Extension Header

Modo Transporte

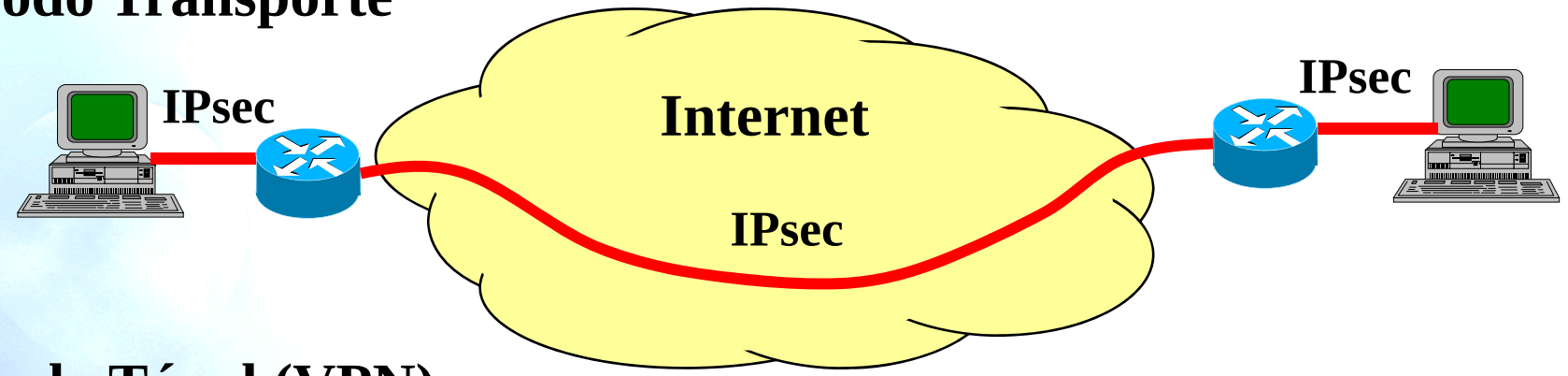


Modo Túnel

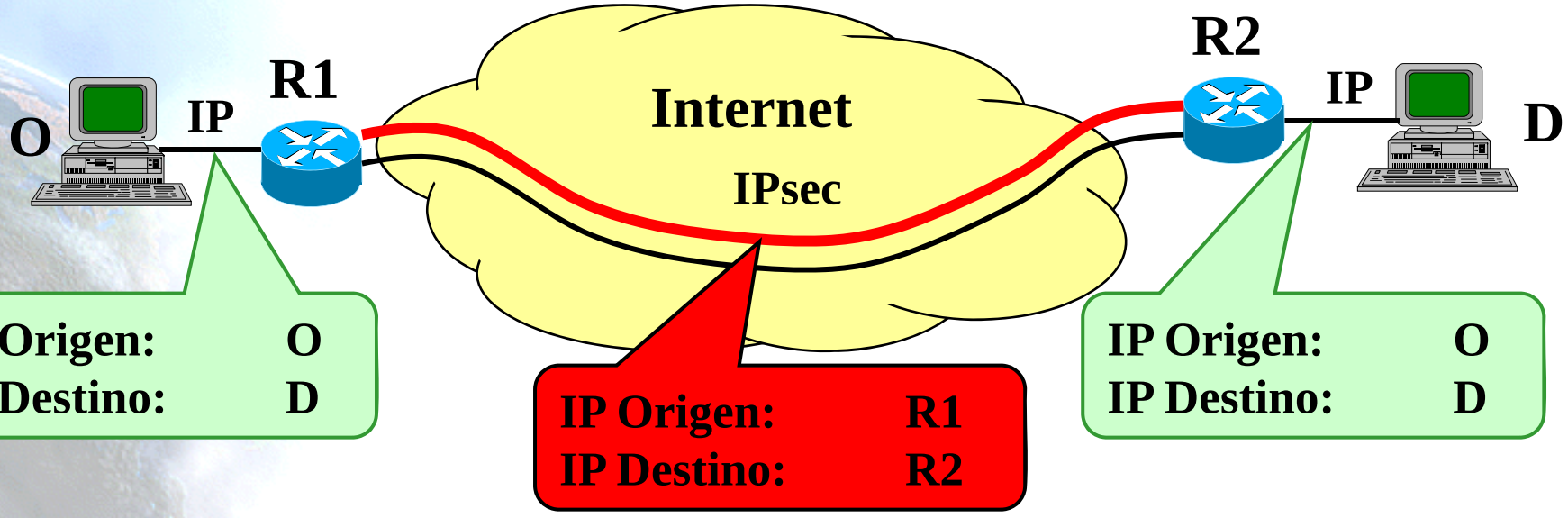


Modo Transporte vs. Túnel

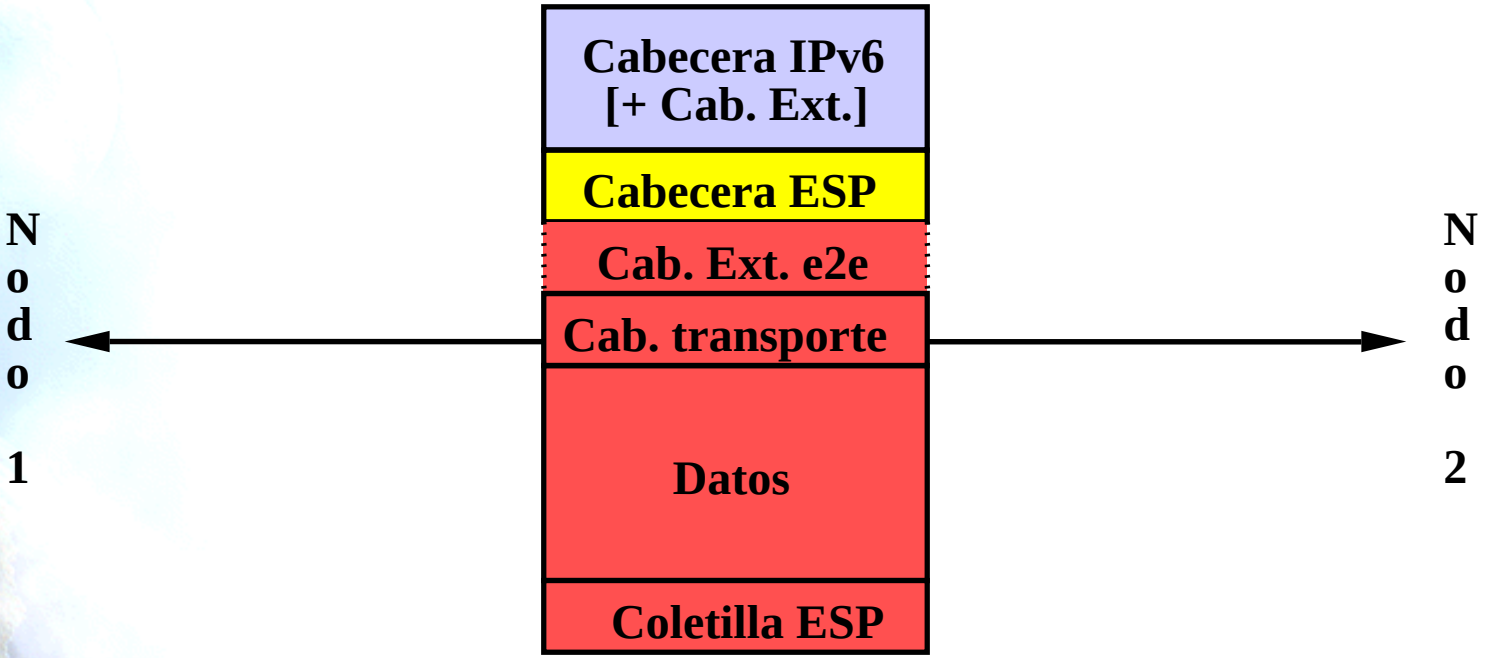
Modo Transporte



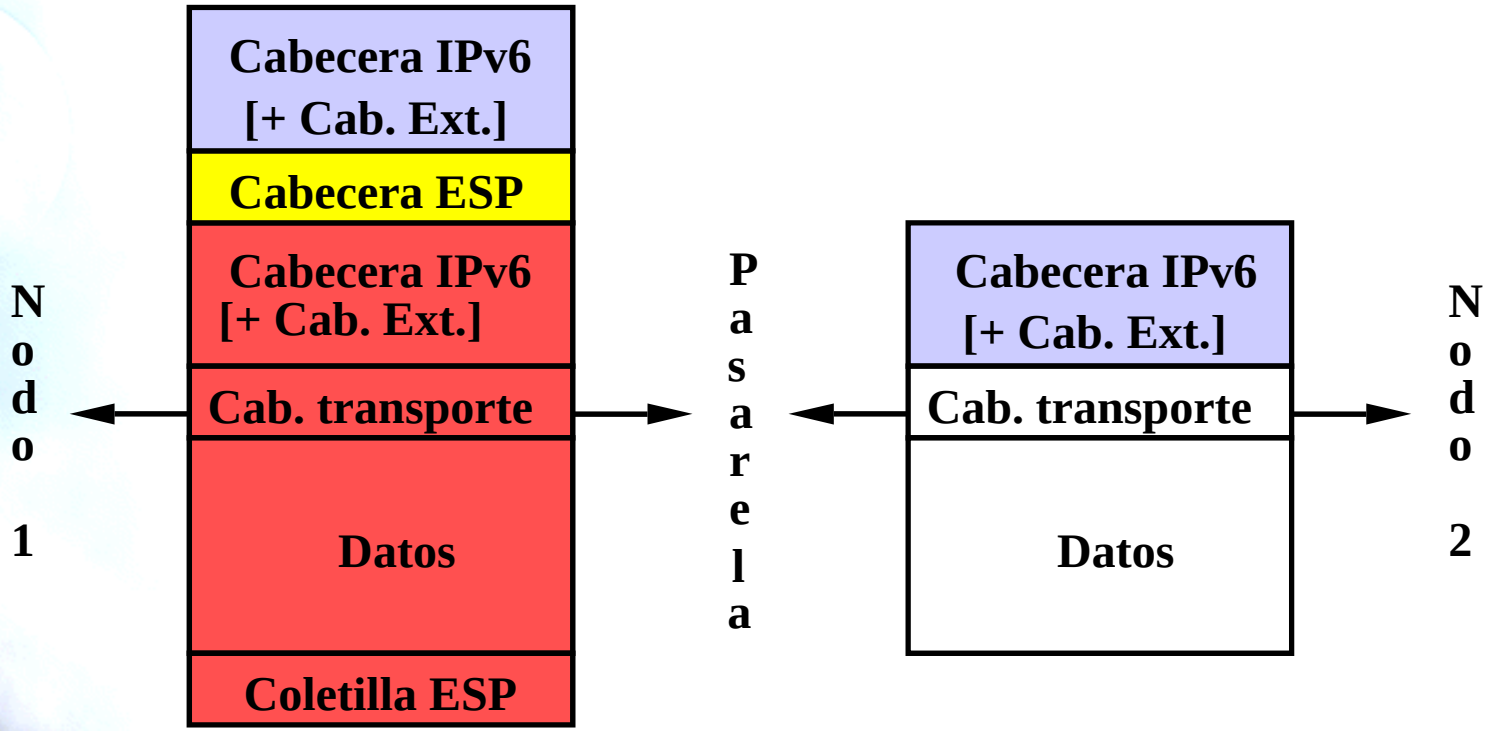
Modo Túnel (VPN):



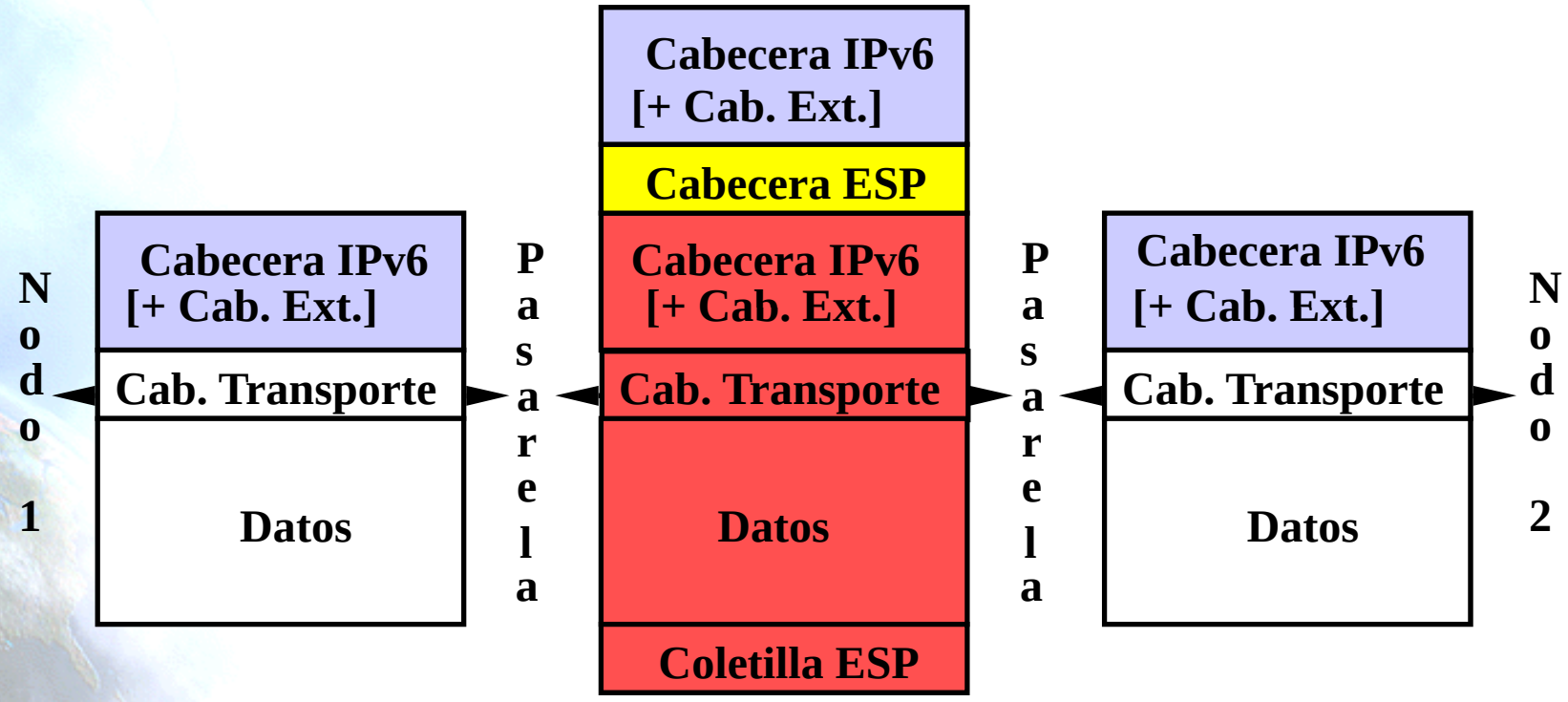
ESP Modo Transporte Extremo-a-extremo



ESP Modo Túnel
Extremo a Pasarela de Seguridad



ESP Modo Túnel
Pasarela a Pasarela



El problema de la clave

- AH y ESP necesitan usar las mismas claves con el fin de establecer la SA entre los nodos extremos
  - En algunos casos esa clave se configura manualmente, pero no es una solución escalable a decenas o cientos de nodos
    - Gestión más sencilla.
    - Cada sistema se configura con las claves propias y de los demás.
  - En ciertos entornos se necesita una solución que sea automática, creando una SA de forma dinámica, pero eso requiere la existencia de un canal seguro entre los nodos con el fin de intercambiar las claves
    - IKE es la solución propuesta para el establecimiento de SA de forma automática
- IKEv1 (RFC4109) es en realidad una combinación de otras piezas:
  - ISAKMP (RFC2408). Marco abstracto para la autenticación e intercambio de claves, diseñado para ser independiente del método particular de intercambio de claves que se vayan a usar
    - “Internet IP Security Domain of Interpretation for ISAKMP” o Internet DOI (RFC2407). Define el uso de los campos de ISAKMP (números de protocols, algoritmos, modos, etc.)
  - OAKLEY (RFC2412). Proporciona métodos seguros para la determinación de claves.
  - SKEME. Proporciona un mecanismo versátil para el intercambio de claves.

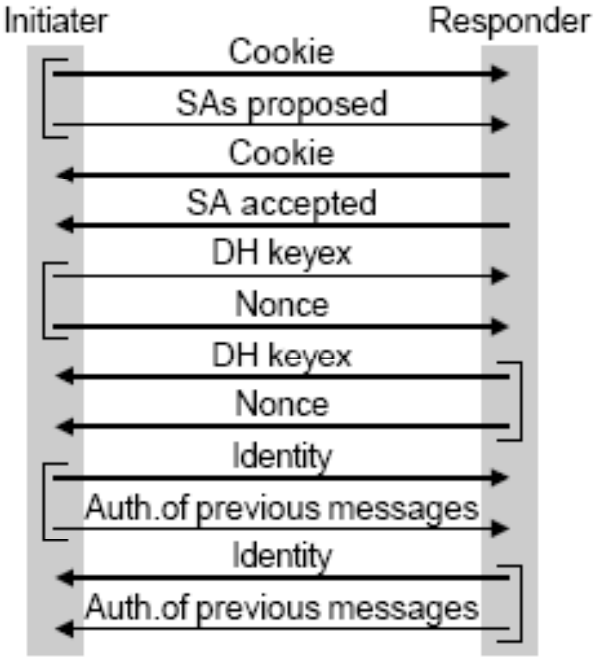
Principios básicos de IKE (1)

- “IKE proporciona un mecanismo seguro para el intercambio de claves entre nodos Ipsec con el fin de permitir el establecimiento y gestión de SA
  - Se trata de un protocolo extremo-a-extremo
  - El bloque fundamental de IKE es la Asociación de Seguridad del protocolo ISAKMP
    - Una SA ISAKMP es bidireccional, a diferencia de una SA IPsec
- IKE proporciona un canal seguro para el intercambio de información para el establecimiento de claves para IPsec
- Los nodos involucrados deben autenticarse mutuamente mediante:
  - “pre-shared secrets” (PSK)
  - Firmas digitales (DSS o RSA)
  - Certificados X.509
  - Encriptación basada en claves públicas
- IKE usa datagramas UDP para el intercambio de mensajes
  - Puerto 500
- La configuración ISAKMP se compone de dos fases
  - La fase 1 es para la configuración de una SA ISAKMP entre los dos nodos (canal seguro)
    - Se ejecuta de forma infrecuente
    - Existen tres modos diferentes de funcionamiento de la fase 1 apropiados para diferentes escenarios/servicios
  - La fase 2 sirve para el establecimiento de la asociación IPsec
    - Se ejecuta más a menudo para generar otras SAs

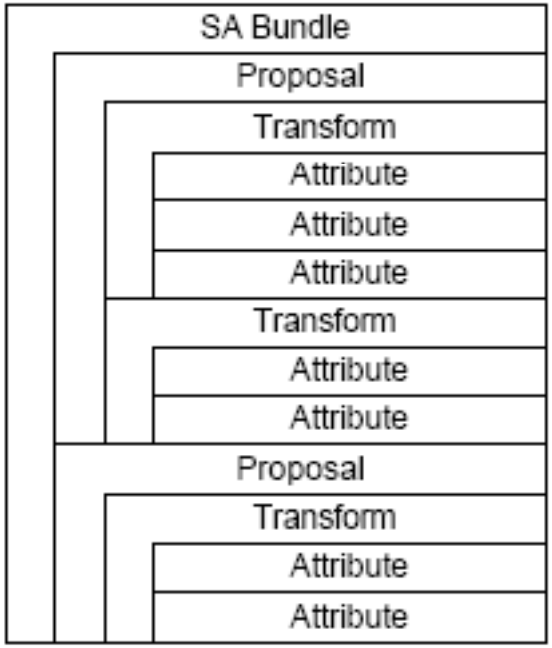
Principios básicos de IKE (2)

- Existen muchísimas variantes posibles debido a las posibles variantes de parámetros
  - Tipos de algoritmos de cifrado
  - Tipos funciones hash
  - Tipos algoritmos intercambio de claves
  - Tipos de autenticación
- ISAKMP se base en valores de jerarquía multinivel
  - Cada propuesta se compone de una transformada con diferentes atributos
  - Cada transformada define
    - Método de cifrado
    - Método de autenticación

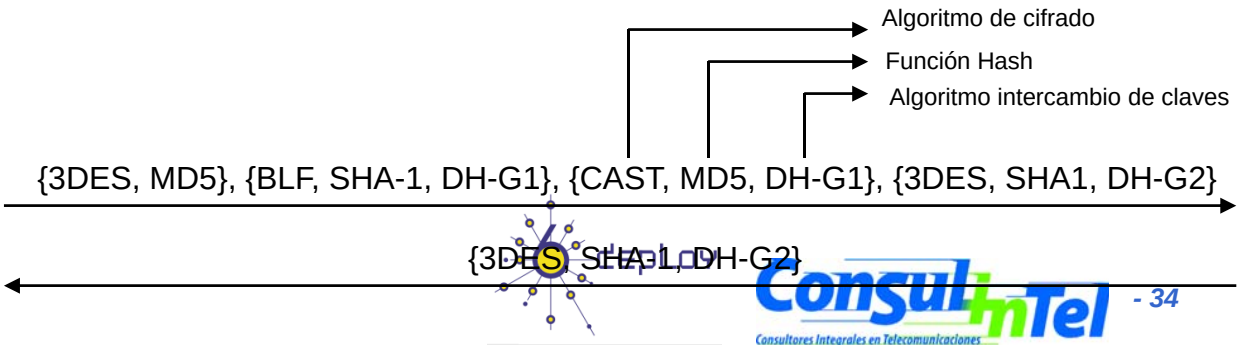
Ejemplo de FASE1



Ejemplo de SA ISAKMP



Ejemplo de negociación de parámetros de seguridad



Objetivos de IKEv2

- IKEv1 es demasiado difícil y extremadamente complicado de depurar en caso de problemas
- IKEv1 no es manejable en entornos de producción con muchos nodos
- La configuración de IKEv1 precisa de ingenieros de red con mucha experiencia
  - Se puede llegar a tardar más de una jornada de trabajo en la configuración de un enlace IPsec con IKEv1 en el caso de usar equipos de fabricantes diferentes
- Al final los usuarios tienden a configurar manualmente las SA IPsec debido a la complejidad de IKEv1
- Como consecuencia se ha definido IKEv2 (RFC4306) con el fin de hacer las cosas más sencillas
  - IKEv2 se define en un solo documento en vez de un conjunto de ellos como en IKEv1
  - Con IKEv2 se simplifica y se mejora IKEv1
  - IKEv2 ofrece un formato de cabeceras y un intercambio de mensajes más simple que IKEv1
  - Soluciona varios problemas de IKEv1

Diferencias de IKEv2 respecto IKEv1

- La principal es que tiene muchas funcionalidades en común con IKEv1 pero de forma más simple:
  - Ocultación de la identidad
  - “perfect forward secrecy” (PFS)
  - Dos fases para el establecimiento de la SA
  - Negociación de las claves
  - IKEv2 usa también el puerto 500 UDP para el intercambio de mensajes, pero **NO** es compatible con los mensajes de IKEv1
- IKEv2 pone más énfasis en VPN (modo túnel)
- Proporciona la posibilidad de atravesar NATs
  - Permite el encapsulamiento de paquetes IKE y ESP en UDP para atravesar NATs
- Su funcionamiento se basa en conocer el estado de la conexión con el fin de prevenir ataques de tipo DoS
- Se añade soporte EAP (RFC2284) como método de autenticación
- Se permite una asignación dinámica de dirección IP posibilitando la actualización de la SA
- Se permite el uso de compresión IP
- Buen soporte para la integración con infraestructuras AAA con el fin de que todo el material criptográfico del usuario resida en dicha infraestructura

5.3 Extensiones de Privacidad

Introducción

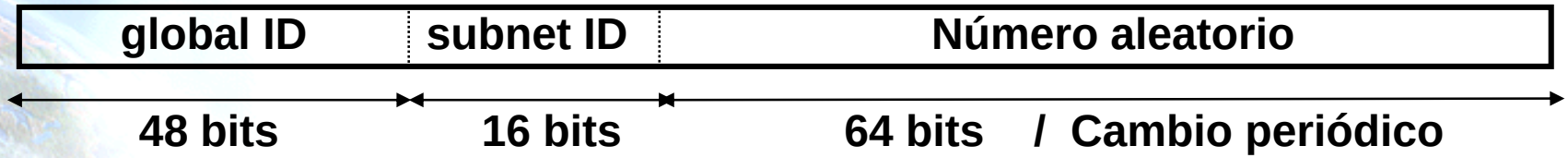
- En la autoconfiguración “stateless” de IPv6 en algunos casos el identificador de interfaz contiene un identificador único del IEEE, lo que permite identificar un nodo a partir de una dirección IP.
- El RFC4941 describe una extensión para la autoconfiguración “stateless” en IPv6 que hace que los nodos generen direcciones de ámbito global que cambian con el tiempo.
- El RFC4941 se basa en generar identificadores de interfaz aleatorios con un tiempo de vida limitado.

¿Por qué Extensiones de Privacidad?

- El problema (con identificadores IEEE)
  - Las direcciones IPv6 en un interfaz dado y generada via “Stateless Autoconfiguration” contienen el mismo ID de interfaz, con independencia del lugar de Internet en el que el dispositivo se conecta. Esto puede facilitar la trazabilidad de dispositivos y/o individuos.
- Posibles Soluciones
  - Usar DHCPv6 para obtener direcciones. El servidor DHCP podría asignar “direcciones temporales” que nunca se renuevan y tienen la condición de temporalidad necesaria
  - Cambiar el ID de interfaz de una dirección IPv6 cada cierto tiempo y generar por tanto nuevas direcciones IPv6 para determinados ámbitos

Extensiones de Privacidad (1)

- Los nodos usan “IPv6 Stateless Autoconfiguration” para generar direcciones sin la necesidad de usar un servidor DHCPv6
  - Las direcciones se forman combinando el prefijo de red con un ID de interfaz
    - En interfaces que contienen ID de IEEE, se usa dicho ID para derivar el ID de interfaz de la dirección IPv6
    - En otros tipos de interfaces, el ID se crea por otros medios, por ejemplo generando números aleatorios



- El uso de extensiones de privacidad hace que los nodos generen direcciones IPv6 partiendo de ID de interfaz que cambian de vez en cuando, incluso si el interfaz contiene un ID de IEEE

Extensiones de Privacidad (2)

1. En realidad no provoca ningún cambio en el comportamiento básico de las direcciones generadas vía “Stateless Autoconfiguration”.
2. Se crean direcciones adicionales basadas en un ID de interfaz aleatorio con el propósito de iniciar sesiones.
   - Estas direcciones aleatorias se suelen emplear durante un período corto de tiempo (desde horas a días) y son deprecadas después de dicho período.
   - Las direcciones deprecadas se pueden seguir usando para sesiones abiertas, pero no para iniciar nuevas conexiones.
   - Periódicamente se generan nuevas direcciones temporales para reemplazar direcciones temporales que ya han expirado.
3. Se produce una secuencia de direcciones globales temporales a partir de una secuencia de IDs de interfaz que aparentemente son aleatorios en el sentido de que es difícil para un observador externo predecir la dirección/identificador futura basada en la actual e igualmente difícil determinar la dirección anterior conociendo la presente.
4. Por defecto, a partir del mismo ID de interfaz aleatorio, se generan tantas direcciones como prefijos se hayan usado para generar una dirección global mediante SAAC.

5.4 Amenazas a ND

Visión General

- El protocolo Neighbor Discovery (ND) (RFC4861) es vulnerable a diversos ataques (RFC3756)
- La especificación original del protocolo ND define el uso de IPsec para proteger los mensajes de ND. Por diversas razones en la práctica esta no es una solución
- SEcure Neighbor Discovery (SEND) (RFC3971), explicado anteriormente, tiene como objetivo proteger ND

Amenazas a ND (1)

- Neighbor Solicitation/Advertisement Spoofing
  - Se hace o bien mandando un NS con una opción de dirección de capa de enlace origen cambiada, o enviando un NA con una opción de dirección de capa de enlace destino cambiada
  - Este es un ataque de redirección/DoS
- Fallo de Neighbor Unreachability Detection (NUD).
  - Un nodo malicioso puede permanecer enviando NAs hechos “a medida” como respuesta a mensajes NS de NUD. Si los mensajes NA no se protegen de alguna manera el atacante puede llevar a cabo el ataque por periodos muy largos de tiempo
  - Este es un ataque DoS (Denegación de Servicio)

Amenazas a ND (2)

- Ataque DoS usando DAD
  - Un nodo atacante puede lanzar un ataque DoS respondiendo a todos los intentos de DAD hecho por un host que llega a la red
  - El atacante puede reclamar la dirección de dos maneras: puede responder con un NS, simulando que también esta haciendo DAD, o bien puede responder con un NA, simulando que ya ha esta usando esa dirección
  - También puede estar presente cuando se use otro tipo de configuración de direcciones, es decir, siempre que se invoque DAD antes de configurar una dirección
  - Es un ataque de tipo DoS

Amenazas a ND (3)

- Encaminador de Último Salto Malicioso
  - Un nodo atacante en la misma subred que un host que intenta descubrir un encaminador de ultimo salto legítimo, se puede hacer pasar por un encaminador IPv6 enviando por multicast un RA o por unicast un RA como respuesta a un RS del nodo que llega a la red
  - El atacante se puede asegurar de que el nodo que llega a la red lo selecciona a él como el encaminador por defecto enviando periódicamente por multicast RAs para el encaminador verdadero pero con tiempo de vida cero. Esto haría que creyese que el router verdadero no quiere cursar tráfico
  - Esta amenaza es un ataque de redirección/DoS

Amenazas a ND (4)

- ‘Muerte’ del encaminador por defecto
  - Un atacante ‘mata’ el(los) encaminador(es) por defecto, haciendo que todos los nodos del enlace asuman que todos los nodos son locales
  - El atacante puede lanzar un ataque DoS clásico contra el encaminador de forma que parezca que no responde. Otra forma sería enviar un RA falso con tiempo de vida cero (zero Router Lifetime)
- El ‘buen’ encaminador se vuelve ‘malo’
  - Un router en el que previamente se confiaba queda comprometido
  - Se aplica el caso de ‘Encaminador de último salto malicioso’
  - Este es un ataque de redirección/DoS

Amenazas a ND (5)

- Mensaje Redirect Falso
  - El atacante usa la dirección en enlace-local del encaminador de primer salto actual para enviar un mensaje Redirect a un host legítimo
  - Debido a que el host identifica el mensaje como proveniente del encaminador por la dirección de enlace-local, acepta el Redirect
  - Siempre que el atacante responda a los mensajes NUD a la dirección de capa de enlace, el efecto de la redirección seguirá vigente
  - Este es un ataque de redirección/DoS

Amenazas a ND (6)

- Prefijo falso en el enlace
  - Un nodo atacante puede enviar un RA especificando que un prefijo de longitud arbitraria pertenece al enlace
  - Si un host que va a enviar un paquete piensa que ese prefijo pertenece al enlace, nunca enviará un paquete con destino a ese prefijo al encaminador. Por el contrario, usará un NS para resolver la dirección, pero el NS no tendrá respuesta, denegando de esta forma el servicio a ese host
  - Este ataque se puede extender a un ataque de redirección si el atacante responde al NS con NAs falsos
  - Este es un ataque DoS

Amenazas a ND (7)

- Prefijo falso para configuración de dirección
  - Un nodo atacante puede enviar un RA especificando un prefijo de red inválido para ser usado por un host para la autoconfiguración de direcciones
  - Como resultado, los paquetes de respuesta nunca llegan al host porque su dirección origen no es valida
  - Este ataque tiene el potencial de propagarse más allá del host atacado si el host realiza una actualización dinámica en el DNS usando la dirección construida con el prefijo falso
  - Este es un ataque DoS

Amenazas a ND (8)

- Parámetros falseados.
  - Un nodo atacante puede enviar RAs con significado válido que dupliquen los RAs enviados por el encaminador por defecto válido, excepto en que los parámetros incluidos están pensados para interrumpir el tráfico legítimo
  - Algunos ataques específicos:
    1. Incluir un 'Current Hop Limit' de uno u otro número pequeño que el atacante sepa causará que los paquetes legítimos se descartarán antes de llegar a su destino
    2. El atacante implementa un servidor o 'relay' DHCPv6 falso y los flags 'M' y/o 'O' están activados, indicando que la configuración 'stateful' de direcciones y/o otros parámetros de realizarse. El atacante puede responder a las peticiones de configuración 'stateful' de un host legítimo con sus respuestas falsas
  - Este es un ataque DoS

Amenazas a ND (9)

- Ataques de Reactuación (Replay)
  - Todos los mensajes de Neighbor Discovery y Router Discovery pueden sufrir ataques de reactuación
  - Un atacante podría capturar mensajes válidos y reenviarlos más tarde
  - En los intercambios de tipo petición-respuesta, como los de ‘Solicitation-Advertisement’, la petición puede contener un valor (nonce) que debe aparecer también en la respuesta. Las respuestas antiguas no son válidas ya que no contienen el valor correcto
  - Los mensajes ‘solitarios’, como los ‘Advertisements’ no solicitados o los mensajes ‘Redirect’, deben protegerse con sellos temporales o contadores

Amenazas a ND (10)

- Ataque DoS a Neighbor Discovery
  - El nodo atacante comienza a fabricar diversas direcciones a partir del prefijo de red y envía paquetes continuamente a esas direcciones. El encaminador de último salto se ve obligado a resolver esas direcciones enviando paquetes NS
  - Un host legítimo que intenta conectarse a la red no será capaz de obtener servicio de ND por parte del encaminador de último salto ya que estará ocupado enviando otras peticiones (NS)
  - Este ataque DoS es diferente de los otros en el sentido de que el atacante puede estar fuera del enlace

5.5 Comparativa IPv4 vs. IPv6

Visión General

- **Seguridad:** incluye diversos procedimientos, mecanismos, prácticas recomendadas y herramientas
- Con **IPv6** hay muchos puntos que serán los mismos que con IPv4, i.e., son “independientes de IP”. Ejemplo, actualizaciones de firmware y software o riesgos de seguridad a nivel de aplicación
- IPv6 introduce nuevos temas a tener en cuenta. Veremos que estos puntos pueden significar una ventaja o desventaja desde el punto de vista de la seguridad

Seguridad IPv6: primer contacto

- Las dos primeras ideas que vienen a la mente de un responsable de seguridad que despliega IPv6 son:
  1. Se utilizan direcciones globales (existe la excepción de las ULAs), i.e., son alcanzables desde cualquier sitio de Internet, en otras palabras, **no hay NAT**.
  2. Todas la pilas IPv6 deben soportar IPsec, como se ha visto.
- La primera puede dar la falsa impresión de peligro y la segunda la falsa impresión de protección. Se profundizará más en esto después.

Clasificación de las Amenazas de Seguridad

- Se establecen tres categorías para las amenazas de seguridad en IPv6:
  1. Amenazas que ya existían con IPv4 y que tienen un comportamiento similar con IPv6.
  2. Amenazas que ya existían con IPv4 y que presentan novedades con IPv6.
  3. Nuevas amenazas que aparecen con IPv6.

Amenazas IPv4 con comportamiento similar con IPv6

- **Sniffing:** IPsec puede ayudar.
- **Ataques a Nivel de Aplicación**: IPsec puede usarse para perseguir al atacante, aunque introduce problemas para los IDS. También puede usarse protección en el nivel de Aplicación.
- **Dispositivos no autorizados**: Se hacen pasar por conmutadores, encaminadores, puntos de acceso o recursos como servidores DNS, DHCP o AAA.
- **Ataques de 'Hombre-en-el-medio'**: IPsec puede ayudar.
- **Ataques por inundación**.

Amenazas IPv4 con diferente comportamiento con IPv6 (1)

- **Escaneo de Red**: El escaneo de una red típica (/64) en la práctica es más difícil. También los ataques automatizados, por ejemplo gusanos que seleccionan direcciones aleatorias para propagarse, se ven dificultados.
- **Ataques de Amplificación Boradcast (Smurf)**: Ataque DoS. Un mensaje echo ICMP se envía a la dirección de broadcast de un prefijo de red con la dirección de origen falseada a la del host víctima. Todos los nodos del prefijo destino envían una echo reply a la víctima. E**n IPv6, no existe el concepto de broadcast.**

Amenazas IPv4 con diferente comportamiento con IPv6 (2)

- **Ataques relacionados con Mecanismos de Transición**: No se utilizan nuevas tecnologías, el mismo tipo de vulnerabilidades que con IPv4:
  - Redes doble-pila pueden ser atacadas usando ambos protocolos.
  - Los túneles IPv6 necesitan nuevos puertos abiertos en los firewalls.

  Recomendaciones:

  - En redes/hosts de doble-pila usar medidas de seguridad similares para IPv4 e IPv6.
  - Controlar el uso de túneles cuando sea posible.
  - Habilitar que los firewalls inspeccionen el tráfico encapsulado.

Nuevas Amenazas IPv6

- Amenazas a ND
- Routing Header Type 0 (RFC5095)
- Mecanismos de Transición, en el sentido de que funcionan encapsulando tráfico y los firewalls y otros dispositivos/software de seguridad deben ser capaces de procesarlos.
- IPsec, en el sentido de enviar datos cifrados que los firewalls no pueden inspeccionar, especialmente firewalls ‘full-state’.

5.6 Aspectos de seguridad con IPv6

Aspectos de Seguridad con IPv6 (1)

- **IPsec**: Como se ha dicho antes es obligatorio en todas las implementaciones de IPv6. Esto puede proporcionar una falsa sensación de seguridad, porque la seguridad la proporciona solamente si se usa IPsec. En la práctica IPsec no se encuentra ampliamente desplegado y en uso debido a la falta de un mecanismo de intercambio de claves a nivel de todo Internet.

  IPsec se configura manualmente para algunas configuraciones concretas y controladas, esto no es escalable.

  Otro aspecto a tener en cuenta es que el tráfico IPsec (ESP) no puede ser inspeccionado por los firewalls.

Aspectos de Seguridad con IPv6 (2)

- **Extrema-a-extremo**: El uso de direcciones IPv6 globales **permite pero no obliga** a todos los nodos a ser alcanzables. El administrador de seguridad/red debe decidir si todos, algunos o ningún tráfico puede alcanzar cada parte de la red.

  Diversos escenarios:

  – **Usuario DSL**: El tráfico debe alcanzar el CPE sin interferencias. El usuario tiene la responsabilidad de filtrar en el CPE.

  – **Centro de Datos**: Entorno controlado donde solo los servicios permitidos deben desplegarse.

Aspectos de Seguridad con IPv6 (3)

- El **nuevo esquema de direccionamiento** implica:
  - El **número de direcciones e**s REALMENTE grande. No tiene sentido el escaneo aleatorio o por fuerza bruta (RFC5157)
  - Cada nodo puede tener **varias direcciones** e incluso identificadores de interfaz aleatorios (RFC4941). Esto dificulta el control sobre un host por medio de su IP
  - El uso de direcciones de enlace-local en una interfaz IPv6, proporciona conectividad IP en un segmento de LAN sin ayuda externa. Como guía, no debe confiarse en sesiones que vengan de direcciones de enlace-local y permitirlas solo para servicios básicos
  - Se han definido direcciones multicast bien conocidas para facilitar la localización de servicios. Esto también facilita la localización de servicios para atacarlos (FF05::2 All routers, FF05::1:3 All DHCP Servers)

Aspectos de Seguridad con IPv6 (4)

- **Cabeceras de Extension (EH)**: este potente y flexible mecanismo debe tenerse en cuenta por los dispositivos de seguridad, es decir, deben ser capaces de inspeccionar la ‘cadena’ de cabeceras.
- **Fragmentación**: En IPv6 solo los hosts finales pueden fragmentar paquetes. Esto reduce los ataques posibles utilizando solapamiento de fragmentos o fragmentos muy pequeños. Las consideraciones para fragmentos desordenados son las mismas que en IPv4 pero en los nodos finales. Los firewalls no deben filtrar fragmentos de paquetes.

Aspectos de Seguridad con IPv6 (5)

- **Autoconfiguración:** En IPv6 se definen distintos medios para la autoconfiguración. DHCP tiene las mismas consideraciones en IPv4 e IPv6. Neighbor Discovery Protocol tiene varias amenazas (como ARP en IPv4), e IPsec y SEND se pueden usar para añadir seguridad.
- **Movilidad IPv6**: IPv6 facilita el despliegue de Movilidad IP aunque algunos elementos necesarios para un despliegue ‘en el mundo real’ están siendo definidos, incluyendo temas de seguridad.

Aspectos de Seguridad con IPv6 (6)

- **Routing Header:** Type 0 Routing Header (RH0) puede ser usada para lograr amplificación de tráfico sobre un camino remoto con el propósito de generar tráfico DoS.

  Se puede construir un paquete que ‘oscile’ entre dos hosts/routers que procesen RH0 muchas veces. Esto permite que un flujo de paquetes de un atacante se amplifique en el camino entre dos encaminadores remotos. Esto puede usarse para causar congestión sobre un camino remoto arbitrario y por lo tanto actuar como un mecanismo de DoS.

Aspectos de Seguridad con IPv6 (7)

- La gravedad de esta amenaza se consideró suficiente para prohibir el uso de RH0 (RFC5095)
- Sólo afecta a la cabecera de extensión Routing Type 0, de manera que las especificaciones para la Type 2 siguen siendo válidas, usada en MIPv6

5.7 Temas prácticos

Temas Prácticos (1)

- **ICMPv6 es una parte fundamental de IPv6**. Con IPv4 un filtrado de tipo 'deny_all_ICMP' podía usarse, pero con IPv6 significaría que funcionalidades básicas dejasen de funcionar.

Type - Code	Descripción	Acción
Type 1	Destination unreachable	ALLOW, de entrada para detectar algunos errores
Type 2	Packet too big	ALLOW, necesario para PMTU discovery
Type 3 - Code 0	Time Exceeded	ALLOW
Type 4 - Code 1 y 2	Parameter problem	ALLOW, para detectar algunos errores
Type 128	Echo reply	ALLOW para **depurar la red** o **Teredo**. De entrada se puede permitir limitando la frecuencia. De salida permitir para algunos **servicios conocidos**.
Type 129	Echo request	ALLOW para **depurar la red** o **Teredo**. De salida se puede permitir limitando la frecuencia. De entrada permitir para algunos **servicios conocidos**.
Type 130,131,132,143	Multicast listener	ALLOW si se despliega Multicast y MLD debe atravesar el firewall
Type 133	Router Solicitation	ALLOW si el firewall interfiere en ND
Type 134	Router Advertisement	ALLOW si el firewall interfiere en ND
Type 135	Neighbor Solicitation	ALLOW si el firewall interfiere en ND
Type 136	Neighbor Advertisement	ALLOW si el firewall interfiere en ND
Type 137	Redirect	NOT ALLOW
Type 138	Renumbering	NO TALLOW
Type 139	Node information Query	NOT ALLOW
Type 140	Node information Reply	NOT ALLOW

Temas Prácticos (2)

- Dependiendo del nivel de control y seguimiento que se requiera se deben usar distintos métodos de configuración de direcciones. De más a menos:
  - Direcciones estáticas.
  - Autoconfiguración ‘Stateful’: DHCPv6.
  - Autoconfiguración ‘Stateless’: Identificador de interfaz a partir de la dirección MAC.
  - Autoconfiguración ‘Stateless’: Identificador de interfaz utilizando las extensiones de privacidad.

Temas Prácticos (3)

- Se recomienda **filtrar los prefijos no asignados**. También el tráfico ULA no debe atravesar Internet. Si se despliega Multicast estos prefijos deben permitirse.

IANA es la encargada de asignar los prefijos de direcciones:

- Espacio Direcciones IPv6: http://www.iana.org/assignments/ipv6-address-space

- Asignaciones Globales Unicast IPv6: http://www.iana.org/assignments/ipv6-unicast-address-assignments

- El filtrado puede ser 'grueso' (Permitir 2000::/3 Global Unicast) o fino (2600:0000::/12, 2400:0000::/12, etc.)

Temas Prácticos (4)

- **Utilizar direcciones difíciles de adivinar**, por ejemplo no usar ::1 para encaminadores o servidores, para dificultar el trabajo del atacante.

  Un ejemplo sería, habilitar la autoconfiguración steteless y después usar esa dirección autoconfigurada en una asignación estática. Esta dirección también se configuraría en el DNS

- **Desplegar Ingress Filtering** (RFC2827, RFC3074) de una manera similar a como se hace para IPv4

Temas Prácticos (5)

- Si se utilizan **Mecanismos de Transición**, asegurarse de que el prefijo correspondiente se anuncia y que su tráfico no se filtra

5.8 Firewalling

Introducción

- Basado en todo lo anterior se darán algunas reglas para ser usadas en los firewalls
- Durante algún tiempo IPv4 e IPv6 coexistirán, así que el escenario más probable será que las redes IPv6 sigan el diseño de las redes IPv4, compartiendo dispositivos de seguridad siempre que sea posible

Consejos (1)

- Ser cuidadoso con el filtrado de ICMPv6 (ver RFC4890)
- Desplegar Ingress filtering (igual que debe hacerse con IPv4)
- Las reglas IPv4 e IPv6 coexistirán, hacerlas coherentes (no permitir todo con IPv6/nada con IPv4).
- Asegurarse de que el firewall soporta:
  - Filtrado por dirección origen y destino
  - Procesado de cabeceras de extensión IPv6 (incluida RH0)
  - Filtrado por información de protocolo de capa superior
  - Inspección de tráfico encapsulado

Consejos (2)

- Considerar el filtrado en tres categorías: Plano de Datos, Plano de Gestión y Plano de Control del Encaminamiento.

5.9 Modelo de Seguridad Distribuida

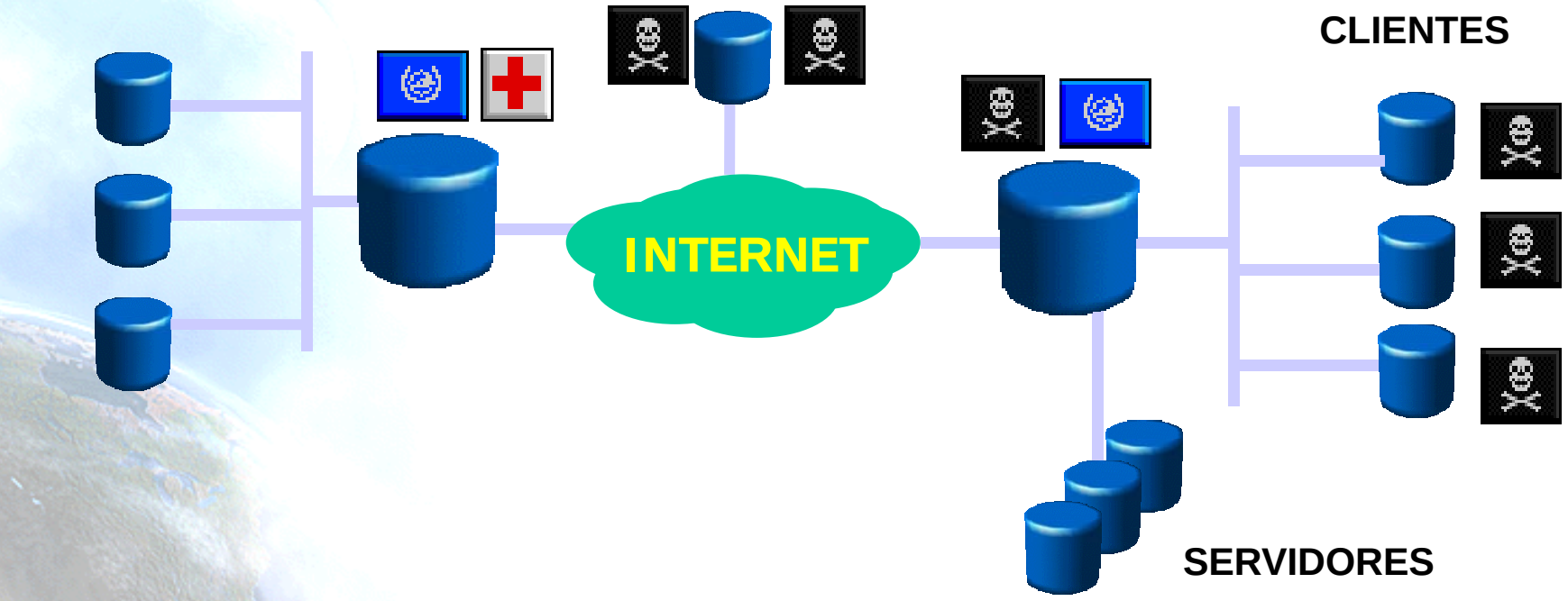
Visión General

- En IPv4 la práctica común es utilizar el **modelo perimetral**, al desplegar seguridad en una red. Este modelo se basa en aislar redes por medio de dispositivos de seguridad a través de los cuales todo el tráfico debe pasar.
- Hoy en día cada vez más herramientas de seguridad se están “moviendo” de la red a los hosts: firewalls, anti-virus, anti-spam, anti-malware, etc.
- Esto conduce al **modelo de seguridad distribuida o de host** en el que la política de seguridad se impone en el host. Esto encaja a la perfección con el modelo extremo-a-extremo que IPv6 ha vuelto a traer.
- También deben tenerse en cuenta los “nuevos” dispositivos IP que usarán las redes IP para conectarse: PDAs, portátiles, domótica, teléfonos móviles, etc. Necesitarán estar protegidos en todas partes!

Consideraciones del Despliegue

- El caso más común es añadir IPv6 a una red IPv4 existente, resultando una red de doble-pila.
- De esta forma nos encontramos con el mismo modelo de seguridad perimetral y dispositivos de seguridad para ser usados en la seguridad IPv6. Esto puede tener algunas ventajas para el personal al cargo y desventajas en caso de falta de soporte IPv6.
- Se espera que en el futuro (próximo) esto cambie debido al despliegue de redes solo IPv6.

Modelo de Seguridad Perimetral (1)

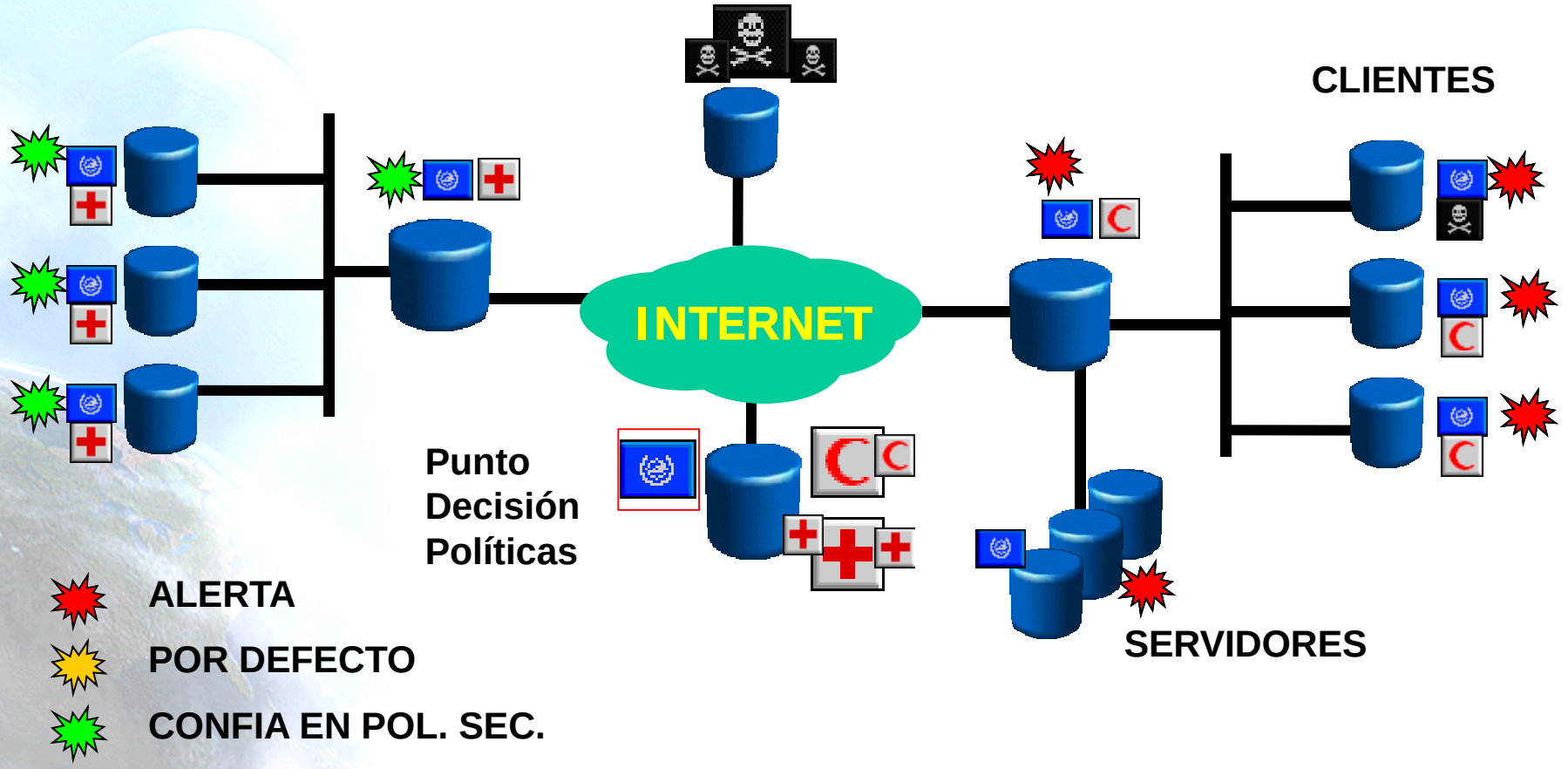


Amenaza Pol. Sec. 1 Pol. Sec. 2 Punto Imposición Política (PIP)

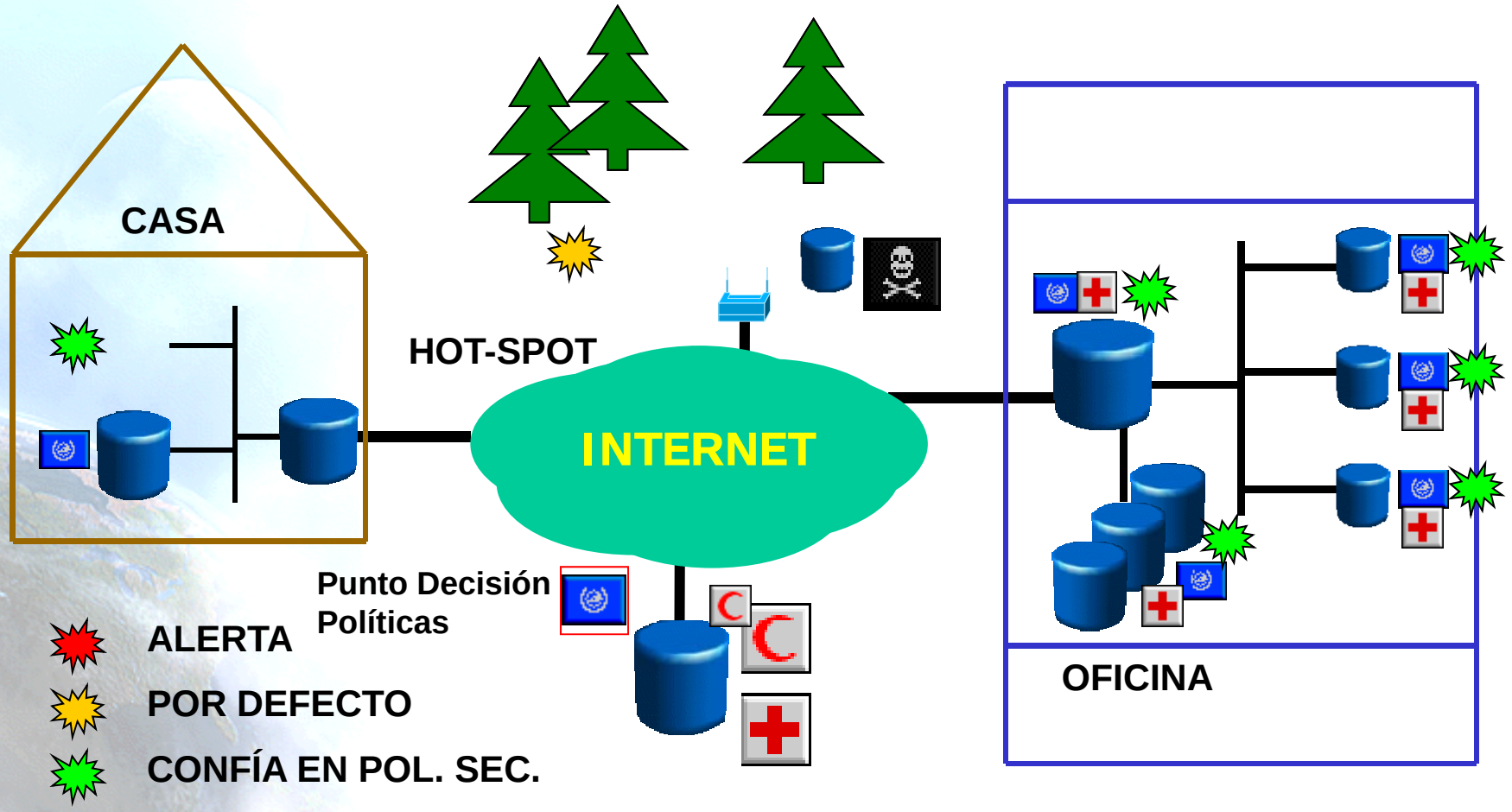
Modelo de Seguridad Perimetral (2)

- La seguridad de un host **depende del punto de la red donde se conecte.**
- **Supuestos principales**:
  - Amenazas vienen de “fuera”.
  - Los nodos protegidos no irán “fuera”.
  - No hay puertas traseras (ADSL, WLAN, etc.).
- **Desventajas principales**:
  - Modelo dependiente del Firewall.
  - No cubre amenazas provenientes de “dentro”.
  - FWs normalmente actúan como NAT/Proxy.
  - Se necesitan soluciones especiales para comunnicaciones seguras en modo transporte.

Modelo de Seguridad Distribuida (1)



Modelo de Seguridad Distribuida (2)



Amenaza Pol. Sec. 1 Pol. Sec. 2 Punto Imposición Política (PIP)

Modelo de Seguridad Distribuida (3)

- **IDEA BÁSICA:** La política de seguridad de define centralmente y de distribuye a los PIPs. Las entidades de red se autentifican para que confíen en ellas.
- **TRES elementos**:
  - Lenguaje de Especificación de Políticas.
  - Protocolo de Intercambio de Políticas.
  - Autentificación de Entidades.
- **Supuestos Principales**:
  - Las amenazas vienen de cualquier parte en la red.
  - Cada host puede ser identificado de forma unívoca y segura.
  - La seguridad se puede aplicar en una o más de las siguientes capas: red, transporte y aplicación.

Modelo de Seguridad Distribuida (4)

- **Desventajas Principales**:
  - Complejidad.
  - Identificación unívoca y segura de hosts no es algo trivial.
  - La actualización de políticas debe llevarse a cabo de una manera eficiente y debe asegurarse que los hosts siguen las políticas.
  - Un host “comprometido” sigue siendo un problema.
  - Es dependiente del Punto de Decisión de Políticas: hay que añadir más complejidad para afrontar esto.

Modelo de Seguridad Distribuida (5)

- **Ventajas principales**:
  - Flexibilidad en la definición de políticas de seguridad
  - Protege contra ataques internos
  - No depende de donde esté conectado el host.
  - Sigue manteniendo un control centralizado.
  - Habilita el modelo de comunicación extremo-a-extremo, tanto seguro como no.
  - Se pueden tomar mejores decisiones basándose en información específica del host.
  - Posibilita una mejor recopilación de información de auditoría.
  - Puede controlar las comunicaciones de un host evitando comportamientos maliciosos en la red local o malas prácticas.
  - Permite desarrollar soluciones de seguridad distribuidas y cooperativas.

Modelo de Seguridad Distribuida(6)

- Existe trabajo en curso que encaja con este modelo:
  1. **Cisco NAC** (Network Access Control): El host debe obtener acceso a la red cumpliendo con una política de seguridad.
  2. **Microsoft NAP** (Network Access Protection): crea políticas para validar la "salud" de un host antes de permitir acceso a la red, actualizar hosts conformes y opcionalmente confinar los host que no cumplan a una red restringida.
  3. **Trusted Network Connect Work Group**: Arquitectura abierta y un conjunto creciente de estándares para la integridad del nodo final.
  4. **IETF NSIS WG**: Trabaja en la dirección de permitir al nodo final, previamente autentificado, a abrir puertos en los firewalls.
  5. **IETF NEA WG**: Revisa el estado de dispositivos finales para monitorizar el cumplimiento de la política de una organización y opcionalmente restringir el acceso hasta que en nodo final se haya actualizado para satisfacer los requisitos.
  6. **IETF IDWG WG** (OLD): define formatos de datos y procedimientos para compartir información de interés a sistema de detección y respuesta de intrusiones, y para sistemas de gestión que pueden necesitar interactuar con ellos.

- El mercado y los estándares parecen ir en la dirección de imponer la política de seguridad en el nodo final por medio del control de acceso a la red.

Gracias !!

Contacto:

- Cesar Olvera (Consulintel): cesar.olvera@consulintel.es
- Alvaro Vives (Consulintel): alvaro.vives@consulintel.es

6DEPLOY Project: http://www.6deploy.org

The IPv6 Portal: http://www.ipv6tf.org