Grupo de Trabajo en Red
Request for Comments: 2407
Categoría: Pila de Estándares
Traducción al castellano:
Hugo Adrian Francisconi

D. Piper
Network Alchemy
Noviembre 1998
Agosto 2005
<adrianfrancisconi@yahoo.com.ar>

El Dominio de Interpretación de Seguridad IP en Internet para ISAKMP

Estado de este documento

Este documento especifica un protocolo de Internet en vías de estandarización, y es susceptible de recibir críticas y sugerencias para su mejora. Vea la edición actual de "Estándares de Protocolos Oficiales de Internet" (STD 1) para conocer el estado de estandarización y status de este protocolo. La distribución de este documento es ilimitada.

Aviso de Copyright

Nota del Grupo de Administración de Ingeniería de Internet (IESG)

La Sección 4.4.4.2 manifiesta que, "Toda implementación dentro del DOI de IPsec DEBE soportar ESP_DES...". Trabajos resientes en el área del análisis criptográfico sugieren que DES puede no ser suficientemente fuerte para muchas aplicaciones. Por consiguiente, es muy probable que el IETF desestime el uso de ESP_DES como un algoritmo criptográfico obligatorio en un futuro cercano. Este permanecerá como de uso opcional en el Protocolo. Aunque el grupo de trabajo de IPsec y el IETF no se han decidido sobre el algoritmo alternativo (hay que tener en cuenta está consideración de seguridad y funcionamiento), implementadores pueden desear tener en cuenta la recomendación de la Sección 4.4.4.3 sobre el uso de ESP_3DES.

1. Resumen

El Protocolo de Gestión de Claves y Asociaciones de Seguridad en Internet (ISAKMP) define un marco para la administración de Asociaciones de Seguridad (SA) y el establecimiento de claves para Internet. Este marco consiste en la definición de intercambios, cargas, y de la elaboración de pautas que suceden dentro de un determinado Dominio de Interpretación (DOI). Este documento define el DOI de Seguridad IP (DOI de IPsec), que lo ejemplifica ISAKMP para usarse con IP cuando IP use ISAKMP para negociar asociaciones de seguridad.

Para una lista de cambios desde la versión anterior del DOI de IPsec, por favor vea la Sección 7.

2. Introducción

Dentro de ISAKMP, un Dominio de Interpretación es usado para relacionar un grupo de protocolos usando ISAKMP para negociar SAs. Los protocolos de seguridad comparten un DOI de protocolo de seguridad elegido y transformaciones criptográficas a partir de un espacio de nombramiento común y de un identificador de protocolo de intercambio de claves común. También comparten la interpretación del DOI especifico de contenido de los datos de la carga, incluyendo la SA y el Identificador de carga.

En general, ISAKMP pone los siguientes requerimientos para una definición de DOI:

- Definir el esquema de nombramiento para los identificadores de protocolo para el DOI específico.
- Definir la interpretación para el campo Situación.
- Definir el conjunto de políticas de seguridad aplicables.
- Definir la sintaxis para los Atributos de las SAs (Fase II) para el DOI específico.
- Definir la sintaxis para los contenidos des las cargas para el DOI específico.
- Definir tipos de Intercambios de Claves adicionales, si es necesario.
- Definir tipos de Mensajes de Notificación adicionales, si es necesario.

El resto del documento detalla las ejemplificaciones de estos requerimientos para usar el protocolo de Seguridad IP (IPsec) para proporcionar autentificación, integrabilidad, y/o confidencialidad para los paquetes IP enviados entre sistemas host y/o firewalls.

Para una descripción global de la arquitectura de IPsec, ver [ARCH], [AH], y [ESP].

3. Definición y Términos

Las palabras DEBE, NO DEBE, REQUERIDO, PODER, NO PODER, DEBERÍA, NO DEBERÍA, RECOMENDADO, PUEDE y OPCIONAL, cuando aparezcan en este documento, deben interpretarse como se describe en [RFC-2119].

4.1 Esquema de Nombramiento IPsec

Dentro de ISAKMP, todos los DOI beben estar registrados por la IANA en el RFC "Números Asignados" [STD-2]. El Número Asignado por la IANA para el DOI de Seguridad IP (DOI de IPsec) es uno (1). Dentro del DOI de IPsec, todos los identificadores bien conocidos DEBEN estar registrados por la IANA bajo el DOI de IPsec. A menos que se mencione lo contrario, todas las tablas de este documento hacen referencia a los Números Asignados por la IANA para el DOI de IPsec. Vea la Sección 6 para información adicional relacionada con el registro de la IANA para el DOI de IPsec.
Todos los valores binarios multi-octetos se almacenan en orden de byte de red.

4.2 Definición de la Situación IPsec

Dentro de ISAKMP, la Situación proporciona información que puede ser usada por el respondedor para elaborar una determinada política sobre como procesar la petición de la SA entrante. Para el DOI de IPsec, el campo Situación es un bitmask de cuatro (4) octetos con los siguientes valores:

Situación	Valor
Situación de solo Identificación (SIT_IDENTITY_ONLY)	0x01
Situación secreta (SIT_SECRECY)	0x02
Situación integridad (SIT_INTEGRITY)	0x04

4.2.1 Situación de solo Identificación (SIT_IDENTITY_ONLY)

El tipo SIT_IDENTITY_ONLY especifica que la SA será identificada por la información de la identidad de origen presente en una Carga de Identificación asociada. Vea la Sección 4.6.2 para una completa descripción de los diversos tipos de Identificadores. Toda implementación DOI de IPsec DEBE soportar SIT_IDENTITY_ONLY para incluir una Carga de Identificación en al menos uno de los intercambios Oakley de la Fase 1 (ver la Sección 5 de [IKE])) y DEBE abortar cualquier instalación de asociación que no incluya una Carga de Identificación.

Si un iniciador no soporta SIT_SECRECY ni SIT_INTEGRITY, la situación consiste solo de la situación bitmap de 4 octetos y no incluye el campo Identificación del Identificador de Dominio (Figura 1, Sección 4.6.1) o ninguna información de identificación posterior. Por el contrario si el iniciador soporta SIT_SECRECY o SIT_INTEGRITY, el campo Identificación del Identificador de Dominio DEBE ser incluido en la carga de situación.

4.2.2 Situación Secreto (SIT_SECRECY)

El tipo SIT_SECRECY especifica que la SA es negociada en un ambiente que requiere identificación de secreto. Si SIT_SECRECY está presente en la situación bitmap, el campo Situación estará seguido por datos de longitud variable que incluyen un nivel de sensibilidad y el sector bitmask. Ver Sección 4.6.1 para una completa descripción del formato de la Carga SA.

Si un iniciador no soporta SIT_SECRECY, SIT_SECRECY NO DEBE ser colocado en la Situación bitmap y no debe ser incluido el nivel de secreto o categorías bitmaps.
Si un respondedor no soporta SIT_SECRECY, una Carga de Notificación conteniendo, Situación No Soportada (SITUATION-NOT-SUPPORTED) DEBERÍA ser enviado y la instalación de la SA DEBE ser abortada.

4.2.3 Situación Integridad (SIT_INTEGRITY)

El tipo SIT_INTEGRITY especifica que la SA es negociada en un ambiente que requiere identificación de integridad. Si SIT_INTEGRITY está presente en la Situación bitmap, el campo Situación estará seguido por datos de longitud variable que incluyen un nivel de integridad y el sector bitmask. Si SIT_SECRECY también es usado en la asociación, la información de integridad estará seguida de los datos del nivel de secreto de longitud variable y de las categorías. Ver Sección 4.6.1 para una completa descripción del formato de la Carga SA.

Si un iniciador no soporta SIT_INTEGRITY, SIT_INTEGRITY NO DEBE ser colocado en la Situación bitmap y no debe ser incluido el nivel de integridad o categorías bitmaps.

Si un respondedor no soporta SIT_INTEGRITY, una Carga de Notificación conteniendo, Situación No Soportada (SITUATION-NOT-SUPPORTED) DEBERÍA ser enviado y la instalación de la SA DEBE ser abortada.

4.3 Requisitos de la Política de Seguridad IPsec

El DOI de IPsec no impone requisitos específicos para la política de seguridad en ninguna implementación. Los asuntos de políticas en sistemas host están fuera del alcance de este documento.

Sin embargo, las subsiguientes secciones tratan algunos de los asuntos que deben ser considerados cuando se diseña una implementación DOI de IPsec en host. Estas secciones deberían ser consideradas solamente de carácter informativo.

4.3.1 Cuestiones Sobre la Gestión de Claves

Se espera que muchos sistemas elijan implementar ISAKMP esforzándose por proporcionar un dominio de interpretación protegido para un conjunto de demonios de administración de claves de IKE. En modo protegido, en sistemas operativos multiusuario, estos demonios de administración de claves, probablemente existan como procesos con privilegios separados.

En tales ambientes, puede ser conveniente que una API (Application Program Interface - Interfase de Programa de Aplicación) realice la introducción del material clave dentro del kernel TCP/IP. La arquitectura de seguridad IP no tiene ningún requerimiento para la estructura o flujo entre un kernel TCP/IP host y estos proveedores de administración de claves.

4.3.2 Cuestiones Sobre las Claves Estáticas

Los sistemas host que implementen claves estáticas, para uso directo de IPsec, o para propósitos de autentificación (ver la Sección 5.4 de [IKE]), deberían tomar medidas para proteger el material clave estático cuando no se encuentre dentro de un área de memoria protegida o cuando lo esté usando el kernel TCP/IP.

Por ejemplo, en una laptop (ordenador portátil), uno podría escoger guardar las claves estáticas en un depósito configurable, es decir, encriptadas bajo una contraseña privada.

Dependiendo del sistema operativo y del software instalado, puede que no sea posible proteger las claves estáticas una vez que estas están dentro del kernel TCP/IP, sin embargo no debería ser banalmente recuperable encender inicialmente el sistema teniendo que satisfacer algunos requerimientos adicionales para la autentificación.

4.3.3 Cuestiones Sobre Política en Host

No es realista asumir que la transmisión IPsec ocurrirá instantáneamente [overnight]. Los sistemas host deben estar dispuestos a implementar listas de políticas flexibles que describan que sistemas desean comunicarse en modo seguro y cuales de ellos requieren comunicaciones en modo seguro.

Una aproximación es probablemente una lista estática de direcciones IP, máscaras de red, y una bandera o banderas con requisitos de seguridad.

Implementaciones más flexibles pueden consistir en una lista de nombres de DNS comodines (por ejemplo, '*.foo.bar'), una máscara de entrada/salida, y direcciones de firewall opcionales. Los nombres de DNS comodines podrían ser usados para hacer corresponder las direcciones IP entrantes o salientes, las máscaras IP podrían ser usadas para determinar si la seguridad será aplicada o no en esa determinada dirección y las direcciones de firewall opcionales podrían ser usadas para indicar si el modo túnel se necesitará o no para comunicarse con el sistema de destino aunque exista un firewall intermedio.

4.3.4 Administración de Certificados

Sistemas host que implementen un esquema de autentificación de certificados necesitarán un mecanismo para obtener y administrar bases de datos de certificados.

Los DNS seguros son uno de los mecanismos de distribución de certificados, no obstante la disponibilidad permanente de zonas con DNS seguros, a corto plazo, es improbable por muchas razones. Lo que es mucho más probable es que los host necesitarán una capacidad para importar los certificados que adquieren a través de mecanismos seguros, mecanismos out-of-band (fuera de banda), así como también una capacidad para exportar sus propios certificados para que lo usen otros sistemas.

Sin embargo, la administración de certificados en forma manual no debería ser realizada para no imposibilitar la capacidad de introducir mecanismos dinámicos de descubrimiento de certificado y/o protocolos cuando sea posible.

4.4 Números Asignados a IPsec

Las siguientes secciones listan los Números Asignados al DOI de IPsec para el: Identificador de Situación, Identificador de Protocolo, Identificador de Transformación AH, Identificador de Transformación ESP, Identificador de Transformación IPCOMP, Valores de los Tipos de Atributos de SA, Identificador de Dominio de Identificación, Valores de Tipos de Identificación de Carga, y Valores de Tipos de Mensajes de Notificación.

4.4.1 Identificador de Protocolo de Seguridad IPsec

La sintaxis de la propuesta de ISAKMP fue diseñada específicamente para contemplar las negociaciones situaciones de de múltiples Fases 2 de conjuntos de protocolos de seguridad dentro de una única negociación. Como consecuencia, la lista de conjuntos de protocolos de abajo forma el conjunto de protocolos que pueden ser negociados al

mismo tiempo. Es una decisión de la política del host qué conjuntos de protocolos pueden ser negociados conjuntamente.

La tabla siguiente lista los valores para los Identificadores de Protocolo de Seguridad referenciados en la Carga de la Propuesta de ISAKMP para el DOI de IPsec.

Identificador de Protocolo	Valor
RESERVADO	0
Protocolo ISAKMP (PROTO_IPCOMP)	1
Protocolo AH IPsec (PROTO_IPSEC_AH)	2
Protocolo ESP IPsec (PROTO_IPSEC_ESP)	3
Protocolo de Compresión IP (PROTO_IPCOMP)	4

4.4.1.1 PROTO_ISAKMP (Protocolo ISAKMP)

El tipo PROTO_ISAKMP especifica que se requiere protección de mensajes durante la Fase 1 de la negociación. El mecanismo de protección específico usado para el DOI de IPsec se describe en [IKE]. Todas las implementaciones dentro del DOI de IPsec DEBEN soportar PROTO_ISAKMP.

NOTA: ISAKMP se reserva el valor uno (1) a través de todas las definiciones del DOI.

4.4.1.2 PROTO_IPSEC_AH (Protocolo AH IPsec)

El tipo PROTO_IPSEC_AH especifica paquetes IP autentificados. La transformación AH por defecto proporciona autentificación del origen de los datos, protección de integridad, y detección de anti-replay. Debido a las consideraciones de control de exportación, la confidencialidad NO DEBE ser proporcionada por ninguna transformación PROTO_IPSEC_AH.

4.4.1.3 PROTO_IPSEC_ESP (Protocolo ESP IPsec)

El tipo PROTO_IPSEC_ESP especifica confidencialidad de paquetes IP. La autentificación si es requerida, debe ser proporcionada como parte de la transformación ESP. La transformación ESP por defecto incluye autentificación del origen de los datos, protección de integridad, detección de anti-replay, y confidencialidad.

4.4.1.4 PROTO_IPCOMP (Protocolo de Compresión IP)

El tipo PROTO_IPCOMP especifica compresión de la carga IP como se define en [IPCOMP].

4.4.2 Identificador de Transformación ISAKMP IPsec

Como parte de una negociación ISAKMP de la Fase 1, la elección del iniciador de ofrecer Intercambios de Claves se hace usando cierta descripción de la política del sistema host. La selección actual de mecanismos de Intercambios de Claves se realiza usando la Carga Propuesta de ISAKMP estándar. La tabla siguiente lista los Identificadores de Transformación de la Fase 1 de ISAKMP definidos por la Carga Propuesta para el DOI de IPsec.

Transformación	Valor
RESERVADO	0
Clave IKE (KEY_IKE)	1

Dentro del marco de ISAKMP y del DOI de IPsec es posible definir protocolos para el establecimiento de claves aparte del IKE (Oakley). Versiones previas de este documento definen tipos de claves manuales y diseños basándose en el uso de un Centro de Distribución de Claves (KDC) genérico. Estos identificadores se han quitado de este documento.

El DOI de IPsec todavía puede ser ampliado para incluir valores adicionales para protocolos de establecimiento de claves no Oakley para ISAKMP y IPsec, tales como Kerberos [RFC-1510] o como el Protocolo de Administración de Claves para Grupos (GKMP) [RFC-2093].

4.4.2.1 KEY_IKE (Clave IKE)

El tipo KEY_IKE especifica el intercambio de claves híbrido ISAKMP/Oakley Diffie-Hellman (IKE) tal como es definido en el documento [IKE]. Todas las implementaciones dentro del DOI de IPsec DEBEN soportar KEY_IKE.

4.4.3 Identificador de Transformación AH IPsec

El Protocolo Cabecera de Autentificación (AH) define una transformación obligatoria y varias trasformaciones opcionales usadas para proporcionar autentificación, integridad y detección de anti-replay. La tabla siguiente lista los Identificadores de Transformación de AH definidos para la Carga Propuesta de ISAKMP para el DOI de IPsec.

Nota: Los atributos del Algoritmo de Autentificación DEBEN ser especificados identificando el apropiado conjunto de protección AH. Por ejemplo, AH_MD5 puede ser interpretado como una transformación AH genérica usando MD5. Para solicitar la construcción de AH con HMAC, se especifica el Identificador de Transformación AH_MD5 junto con el

conjunto de atributos de Algoritmos de Autentificación HMAC-MD5. Esto se ilustra usando la notación "Autentificación (HMAC-MD5)" en las siguientes secciones.

Identificador de Transformación	Valor
RESERVADO	0-1
AH con MD5 (AH_MD5)	2
AH con SHA (AH_SHA)	3
AH con DES (AH_DES)	4

Nota: Todos los algoritmos de implementación obligatorios están listados cómo "DEBEN" ser implementados (por ejemplo AH_MD5) en las siguientes secciones. El resto de los algoritmos son opcionales y PUEDEN ser implementados dentro de cualquier implementación particular.

4.4.3.1 AH_MD5 (AH con MD5)

El tipo AH_MD5 especifica una transformación AH genérica usando MD5. El conjunto de protección actual es determinado de acuerdo con una lista de atributos SA asociados. Una transformación MD5 genérica actualmente no está definida.

Toda implementación dentro de DOI de IPsec DEBE soportar AH_MD5 junto con el atributo Autentificación (HMAC-MD5). Este conjunto es definido como la transformación HMAC-MD5-96 descripta en [HMACMD5].

El tipo AH_MD5 junto con el atributo Autentificación (KPDK) especifica la transformación AH (clave/relleno/datos/clave) descripta en el RFC-1826.

El uso de AH_MD5 junto con algún otro valor de atributo de Algoritmo de Autentificación, actualmente no está definido.

4.4.3.2 AH_SHA (AH con SHA)

El tipo AH_SHA especifica una transformación AH genérica usando SHA-1. El conjunto de protección actual es determinado de acuerdo con una lista de atributos SA asociados. Una transformación SHA genérica actualmente no está definida.

Toda implementación dentro de DOI de IPsec DEBE soportar AH_SHA junto con el atributo Autentificación (HMAC_SHA). Este conjunto es definido como la transformación HMAC-SHA-1-96 descripta en [HMACSHA].

El uso de AH_SHA junto con algún otro valor de atributo de Algoritmo de Autentificación actualmente no está definido.

4.4.3.3 AH_DES (AH con DES)

El tipo AH_DES especifica una transformación AH genérica usando DES. El conjunto de protección actual es determinado de acuerdo con una lista de atributos SA asociados. Una transformación DES genérica actualmente no está definida.

El DOI de IPsec define que AH_DES junto con el atributo Autentificación (DES-MAC) es una transformación DES-MAC. Las implementaciones no requieren soportar este modo.

El uso de AH_DES junto con algún otro valor de atributo de Algoritmo de Autentificación actualmente no está definido.

4.4.4 Identificador de Transformación ESP IPsec

La Carga de Seguridad Encapsulada (ESP) define una transformación obligatoria y varias trasformaciones opcionales usadas para proporcionar confidencialidad a los datos. La tabla siguiente lista los Identificadores de Transformación ESP definidos para la Carga de la Propuesta de ISAKMP para el DOI de IPsec.

Nota: cuando se requiere autentificación, protección de integridad, y detección de anti-replay, los atributos del Algoritmo de Autentificación DEBEN ser especificados para identificar el conjunto de protección ESP apropiado. Por ejemplo, si se requiere la autentificación HMAC-MD5 con 3DES, uno especifica el Identificador de Transformación ESP_3DES con el conjunto de atributos del Algoritmo de Autentificación HMAC-MD5. Para requerimientos de procesamiento adicional, ver la Sección 4.5 (Algoritmos de Autentificación)

Identificador de Transformación	Valor
RESERVADO	0
ESP con DES usando un IV de 64 bits (ESP_DES_IV64)	1
ESP con DES (ESP_DES)	2
ESP con 3DES (ESP_3DES)	3
ESP con RC5 (ESP_RC5)	4
ESP con IDEA (ESP_IDEA)	5
ESP con CAST (ESP_CAST)	6
ESP con BLOWFISH (ESP_BLOWFISH)	7
ESP con 3IDEA (ESP_3IDEA)	8
ESP con DES usando un IV de 32 bits (ESP_DES_IV32)	9
ESP con RC4 (ESP_RC4)	10
ESP con NULL (ESP_NULL)	11

Nota: Todos los algoritmos de implementación obligatorios están listados cómo "DEBEN" ser implementados (por ejemplo ESP_DES) en las siguientes secciones. El resto de los algoritmos son opcionales y PUEDEN ser implementados dentro de cualquier implementación particular.

4.4.4.1 ESP_DES_IV64 (ESP con DES usando un IV de 64 bits)

El tipo ES_DES_IV64 especifica la transformación DES-CBC definida en el RFC-1827 y el RFC-1829 usando un Vector de Inicialización (IV) de 64 bits.

4.4.4.2 ESP_DES (ESP con DES)

El tipo ESP_DES especifica una transformación DES genérica usando DES-CBC. El conjunto de protección actual es determinado de acuerdo con una lista de atributos SA asociados. Una transformación genérica actualmente no está definida.

Toda implementación dentro del DOI de IPsec DEBE soportar ESP_DES junto con el atributo Autentificación (HMAC-MD5). Este conjunto es definido como la transformación [DES], suministrando autentificación y integridad a través de HMAC MD5 [HMACMD5].

4.4.4.3 ESP_3DES (ESP con 3DES)

El tipo ESP_3DES especifica una transformación DES triple genérica. El conjunto de protección actual es determinado de acuerdo con una lista de atributos SA asociados. Una transformación genérica actualmente no está definida.

Toda implementación dentro de DOI de IPsec se le aconseja encarecidamente soportar ESP_3DES junto con el atributo Autentificación (HMAC-MD5). Este conjunto es definido como la transformación [ESPCBC], suministrando autentificación y integridad por HMAC MD5 [HMACMD5].

4.4.4.4 ESP_RC5 (ESP con RC5)

El tipo ESP_RC5 especifica la transformación RC5 definida en [ESPCBC].

4.4.4.5 ESP_IDEA (ESP con IDEA)

El tipo ESP_IDEA especifica la transformación IDEA definida en [ESPCBC].

4.4.4.6 ESP_CAST (ESP con CAST)

El tipo ESP_CAST especifica la transformación CAST definida en [ESPCBC].

4.4.4.7 ESP_BLOWFISH (ESP con BLOWFISH)

El tipo ESP_BLOWFISH especifica la transformación BLOWFISH definida en [ESPCBC].

4.4.4.8 ESP_3IDEA (ESP con 3IDEA)

El tipo ESP_3IDEA esta reservado para IDEA triple.

4.4.4.9 ESP_DES_IV32 (ESP con DES usando un IV de 32 bits)

El tipo ESP_DES_IV32 especifica la transformación DES-CBC definida en el RFC 1827 y en el RFC 1829 usando un Vector de Inicialización (IV) de 32 bits.

4.4.4.10 ESP_RC4 (ESP con RC4)

El tipo ESP_RC4 esta reservado para RC4.

4.4.4.11 ESP_NULL (ESP con NULL)

El tipo ESP_NULL especifica que la confidencialidad no debe ser proporcionada por ESP. ESP_NULL se usa cuando ESP es usado para paquetes tuneliados que solamente requieren autentificación, protección de integridad, y detección de anti-replay.

Toda implementación dentro del DOI de IPsec DEBE soportar ESP_NULL. La transformación ESP NULL se define en [ESPNULL]. Ver la descripción de atributos de los Algoritmos de Autentificación en la Sección 4.5 para requerimientos adicionales relacionados con el uso de ESP_NULL.

4.4.5 Identificador de Transformación IPCOMP IPsec

La transformación de la compresión IP (IPCOMP) define algoritmos de compresión opcionales que pueden ser negociados para proporcionar compresión de la carga IP ([IPCOMP]). La tabla siguiente lista los Identificadores de Transformación IPCOMP definidos para la Carga Propuesta de ISAKMP dentro del DOI de IPsec.

Identificador de Transformación	Valor
RESERVADO	0
IPCOMP_OUI	1
IPCOMP_DEFLATE	2
IPCOMP_LZS	3

4.4.5.1 IPCOMP_OUI

EL tipo IPCOMP_OUI especifica una propiedad de transformación de compresión. El tipo IPCOMP_OUI debe estar acompañado por un atributo que identifique el algoritmo específico del vendedor.

4.4.5.2 IPCOMP_DEFLATE

El tipo IPCOMP_DEFLATE especifica el uso del algoritmo de compresión "zlib" como se especifica en [DEFLATE].

4.4.5.3 IPCOMP_LZS

El tipo IPCOMP_LZS especifica el uso del algoritmo Stac Electronics como se especifica en [LZS].

4.5 Atributos de la Asociación de Seguridad IPsec

Las siguientes definiciones de los atributos de las SAs se usan en la negociación de la Fase 2 de IKE. Los tipos de Atributos pueden ser Básico (B) o Longitud-Variable (V). La codificación de estos atributos es definida en la especificación de ISAKMP.

La descripción de atributos como básico NO DEBE ser codificada como variable. El atributo longitud variable puede ser codificado como atributo básico si su valor puede entrar dentro de dos octetos. Ver [IKE] para información adicional sobre la codificación de los atributos en el DOI de IPsec. Todas las restricciones enumeradas dentro de [IKE] también se aplican al DOI de IPsec.

Tipos de Atributos

Clase	valor	tipo
Tipo de Vida de la SA	1	B
Tiempo de Vida de la SA	2	V
Descripción del Grupo	3	B
Modo de Encapsulación	4	B
Algoritmos de Autentificación	5	B
Longitud de la Clave	6	B
Ciclo de la clave	7	B
Tamaño de la Compresión del Diccionario	8	B
Algoritmo de Compresión Privado	9	V

Clase de Valores

Tipo de Vida de la SA
Tiempo de Vida de la SA

Especifica el tiempo de vida para la SA. Cuando la SA expira, todas las claves negociadas bajo la asociación (AH o ESP) deben ser renegociadas. Los valore para el tipo de vida son:

RESERVADO	0
segundos	1
kilobytes	2

Los valores de 3 a 61439 están reservados por la IANA. Los valores de 61440 a 65535 son para uso privado. Para un Tipo de Vida dado, el valor del atributo del Tiempo de Vida define la longitud actual del componente tiempo de vida -- un número de segundos, o un número en kilobytes que pueden ser protegidos.

Si no se especifica, se asumirá el valor por defecto el cual es de 28800 segundos (8 horas).

Un atributo Tiempo de Vida de la SA siempre DEBE estar seguido de un atributo Tipo de Vida que describa la unidad de duración.

Ver Sección 4.5.4 para información adicional relacionada con la notificación del tiempo de vida.

Descripción del Grupo

Especifica el Grupo Oakley usado en una negociación en QM (Modo Rápido - Quick Mode) PFS (Perfect Forward Secrecy). Para una lista de valores soportados, ver el Apéndice A de [IKE].

Modo de Encapsulación

RESERVADO	0
Túnel	1
Transporte	2

Los valores de 3 a 61439 están reservados por la IANA. Los valores de 61440 a 65535 son para uso privado.

Si no se especifica, se asumirá el valor por defecto como no especificado (depende del host).

Algoritmo de Autentificación

RESERVADO	0
HMAC-MD5	1
HMAC-SHA	2
DES-MAC	3
KPDK	4

Los valores de 5 a 61439 están reservados por la IANA. Los valores de 61440 a 65535 son para uso privado.

No existe valor por defecto para el Algoritmo de Autentificación, se debe especificar para identificar correctamente la transformación AH o ESP aplicada, excepto en los siguientes casos:

Cuando ESP es negociado sin autentificación, el atributo Algoritmo de Autentificación NO DEBE ser incluido en la propuesta.

Cuando ESP es negociado sin confiabilidad, el atributo Algoritmo de Autentificación DEBE ser incluido en la propuesta y el identificador de transformación ESP debe ser ESP_NULL.

Longitud de la Clave

RESERVADO	0

No existe valor por defecto para la Longitud de la Clave, se debe especificar para usar transformaciones de cifrado con longitudes de claves variable. Para los cifrados que tienen

longitud fija, el atributo Longitud de la Clave NO DEBE ser enviado.

Ciclo de la Clave
RESERVADO 0

No existe valor por defecto para el Ciclo de la Clave, se debe especificar para usar transformaciones de cifrado con un número variable de ciclos.

Tamaño de la Compresión del Diccionario
RESERVADO 0

Especifica el tamaño máximo de longitud del diccionario.

No existe valor por defecto para el tamaño del diccionario.

Algoritmo de Compresión Privado

Especifica un algoritmo de compresión de un vendedor privado. Los primeros tres (3) octetos deben ser una asignación del IEEE company_id (OUI). Los siguientes octetos pueden ser un subtipo específico de la compresión del vendedor, seguido de cero o más octetos de datos del vendedor.

4.5.1 Soporte de Atributo Requerido

Para garantizar interoperatividad, toda implementación DEBE estar preparado para negociar los siguientes atributos:

Tipo de Vida de la SA
Tiempo de Vida de la SA
Algoritmo de Autentificación

4.5.2 Desglosamiento de Atributo Requerido (Tiempo de Vida)

Para permitir flexibilidad en la semántica, el DOI de IPsec REQUIERE que una implementación ISAKMP desglose correctamente una lista de atributos que contengan múltiples instancias de la misma clase de atributo, siempre que las entradas de diferentes atributos no estén en conflicto con la de alguna otra. Actualmente, el único atributo que requiere este tratamiento es el Tipo de Vida y el Tiempo de Vida.

Para comprender por qué esto es importante, el siguiente ejemplo muestra la codificación en binario de una lista de 4 atributos de entrada que especifica un Tipo de Vida de la SA en 100MB o 24 horas. (Ver la Sección 3.3 de [ISAKMP] para una completa descripción del formato de codificación de los atributos.)

```
Attribute #1:
  0x80010001  (AF = 1, type = SA Life Type, value = seconds)

Atributo N°1:
  0x80010001  (AF = 1, tipo = Tipo de Vida de la SA, valor =
               segundos)

Atributo N°2:
  0x00020004  (AF = 0, tipo = Tiempo de Vida de la SA, longitud = 4
               bytes)
  0x00015180  (valor = 0x15180 = 86400 segundos = 24 horas)

Atributo N°3:
  0x80010002  (AF = 1, tipo = Tipo de Vida de la SA, valor = KB)

Atributo N°4:
  0x00020004  (AF = 0, tipo = Tiempo de Vida de la SA, longitud = 4
               bytes)
  0x000186A0  (valor = 0x186A0 = 100000KB = 100MB)
```

Nota: AF = Formato del Atributo

Si se detecta conflicto en los atributos, una Carga de Notificación conteniendo, ATRIBUTOS NO SOPORTADOS DEBERÍA ser enviado y la instalación de la SA DEBE ser abortada.

4.5.3 Negociación del Atributo

Si una implementación recibe una atributo DOI de IPsec especifico (o valor del atributo) el cual no es soportado, una Carga de Notificación conteniendo, ATRIBUTOS NO SOPORTADOS, DEBERÍA ser enviado y la instalación de la SA DEBE ser abortada, amenos que el valor del atributo este dentro del rango reservado.

Si una implementación recibe un valor de atributo dentro del rango reservado, una implementación PUEDE elegir continuar basándose en la política local.

4.5.4 Notificación del Tiempo de Vida

Cuando un iniciador ofrece un tiempo de vida para la SA mayor que lo que el respondedor desea basándose en su política local, el respondedor tiene 3 opciones: 1) cancelar la negociación entrante; 2) completar la negociación pero usando un tiempo de vida más pequeño que el que se había ofrecido; 3) completar la negociación y enviar un aviso de notificación al iniciador indicando el verdadero tiempo de vida del respondedor. La decisión del respondedor depende de la implementación especifica y/o basándose en la política local.

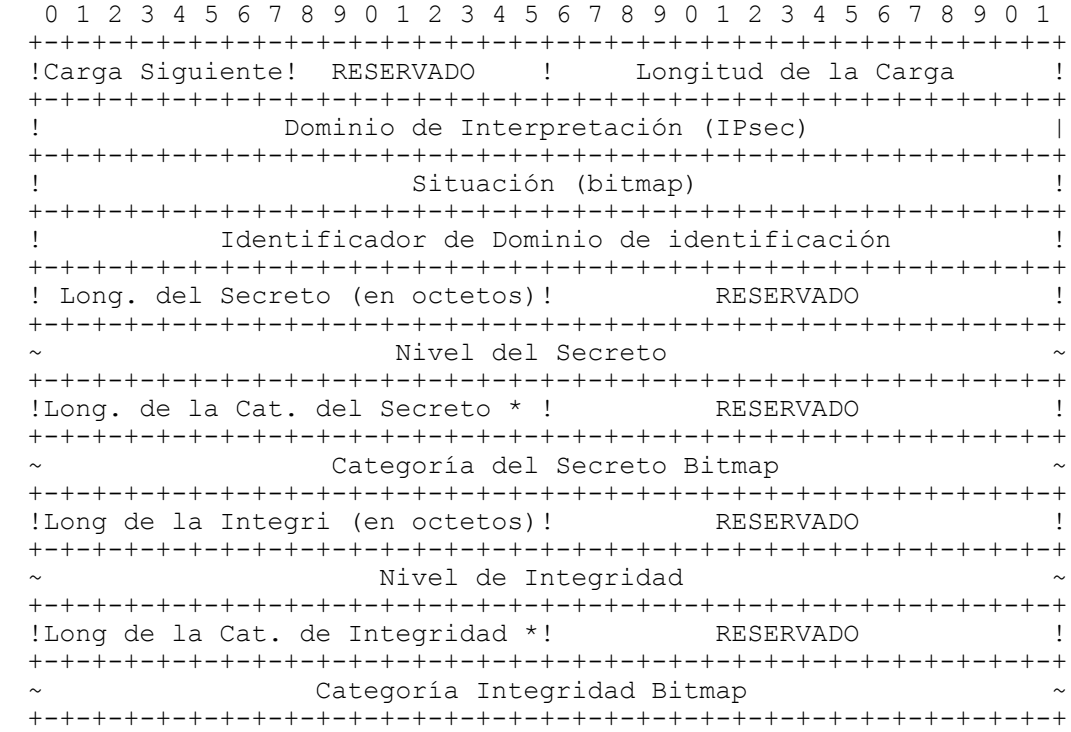
Para garantizar interoperabilidad en el último caso, solamente cuando el respondedor desea notificar al iniciador, el DOI de IPsec requiere que: si el iniciador ofrece un tiempo de vida de la SA mayor de lo que el respondedor está dispuesto a aceptar, el respondedor DEBERÍA incluir una Carga de Notificación ISAKMP en el intercambio que contiene la carga SA IPsec del respondedor. La Sección 4.6.3.1 define el diseño de la carga para el tipo de Mensaje de Notificación Tiempo de Vida del Respondedor (RESPONDER-LIFETIME) el cual DEBE ser usada para este propósito.

4.6 Contenido de la Carga IPsec

Las siguientes secciones describen esas cargas ISAKMP cuya representación de los datos es dependiente del DOI aplicado.

4.6.1 Carga de la Asociación de Seguridad

El diagrama siguiente ilustra el contenido de la Carga SA para el DOI de IPsec. Ver la Sección 4.2 para una descripción de la Situación bitmap.



* = en bits
Cat. = Categoría; Integri = Integridad; Long = Longitud

Figura 1: Formato de la Carga SA

La Carga de la Asociación de Seguridad se definen como sigue:

- Carga Siguiente (1 octeto): Identificador para el tipo de carga de la carga siguiente en el mensaje. Si la carga actual es la última en el mensaje, este campo valdrá cero (0).

- RESERVADO (1 octeto): No usado, debe ser cero (0).

- Longitud de la Carga (2 octetos): Longitud, en octetos, de la carga actual, incluida la cabecera de carga genérica.

- Dominio de Interpretación (4 octetos): Especifica el DOI de IPsec, el cual ha sido asignado con el valor de uno (1).

- Situación (4 octetos): Bitmask usado para interpretar el resto de la Carga SA. Ver Sección 4.2 para una lista completa de valores.

- Identificador de Dominio de identificación (4 octetos): Número Asignado por la IANA usado para interpretar la información del Secreto y de la Integridad.

- Longitud del Secreto (2 octetos): Especifica la longitud, en octetos, del identificador del nivel de secreto, excluyendo los bits de relleno.

- RESERVADO (2 octetos): No usado, debe ser cero (0).

- Nivel del Secreto (longitud variable): Especifica el nivel de secreto requerido obligatoriamente. El nivel del secreto DEBE ser rellenado con ceros (0) para alinearlo a limites de 32 bit.

- Longitud de la Categoría del Secreto (2 octetos): Especifica la longitud, en bits, de la categoría (sector) bitmap, excluyendo los bits de relleno.

- RESERVADO (2 octetos): No usado, debe ser cero (0).

- Categoría del Secreto Bitmap (longitud variable): Un bitmap usado para designar categorías de secretos (sectores) que se requieren. El bitmap DEBE ser rellenado con ceros (0) para alinearlo a limites de 32 bit.

- Longitud de la Integridad (2 octetos): Especifica la longitud, en octetos, del identificador del nivel de integridad, excluyendo los bits de relleno.

- RESERVADO (2 octetos): No usado, debe ser cero (0).

- Nivel de Integridad (longitud variable): Especifica el nivel de integridad requerido obligatoriamente. El nivel de integridad DEBE ser rellenado con ceros (0) para alinearlo a limites de 32 bit.

- Longitud de la Categoría de integridad (2 octetos): Especifica la longitud, en bits, de la categoría de integridad (sector) bitmap, excluyendo los bits de relleno.

- RESERVADO (2 octetos): No usado, debe ser cero (0).

- Categoría Integridad Bitmap (longitud variable): Un bitmap usado para designar categorías de integridad (sectores) que se requieran. El bitmap DEBE ser rellenado con ceros (0) para alinearlo a limites de 32 bit.

4.6.1.1 Identificadores de Dominio de Identificación de IPsec

La tabla siguiente lista los valores asignados para el campo Identificador de Dominio de Identificación contenidos dentro del campo Situación en la Carga SA.

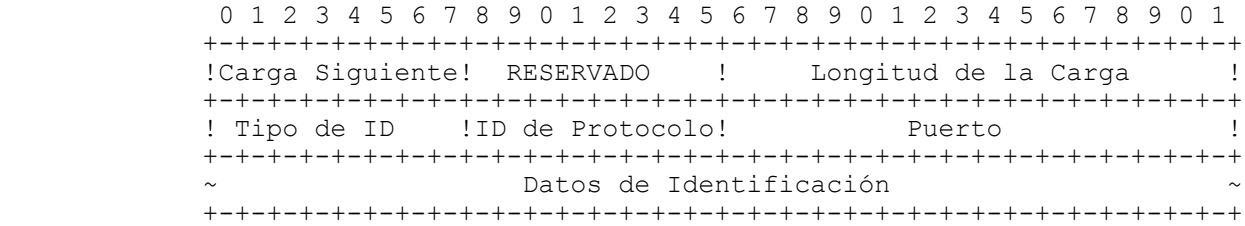
Dominio	Valor
RESERVADO	0

4.6.2 Contenido de la Carga de Identificación

La Carga de Identificación es usada para identificar al iniciador de la SA. La identificación del iniciador DEBERÍA ser usada por el respondedor para determinar los requisitos de la política de seguridad del sistema host adecuados para la asociación. Por ejemplo, un host puede elegir necesitar autentificación y integridad sin confidencialidad (AH) para un cierto conjunto de direcciones IP y brindar autentificación con confidencialidad (ESP) para otro rango de direcciones IP. La Carga de Identificación proporciona información que puede ser usada por el respondedor para tomar esta decisión.

Durante la Fase 1 de la negociación, el campo identificador de protocolo y puerto DEBEN estar en cero o el puerto UDP en 500 [o el campo del puerto debe contener el valor 500] . Si una implementación recibe algún otro valor, este DEBE ser considerado como un error y la carga SA DEBE ser abortada. Este evento DEBERÍA ser auditable.

El siguiente diagrama ilustra el contenido de la Carga de Identificación.



ID = Identificador

Figura 2: Formato de la Carga de Identificación

Los campos de la Carga de Identificación se definen de la siguiente forma:

- Carga Siguiente (1 octeto): Identificador para el tipo de carga de la carga siguiente en el mensaje. Si la carga actual es la última en el mensaje, este campo valdrá cero (0).
- RESERVADO (1 octeto): No usado, debe ser cero (0).
- Longitud de la Carga (2 octetos): Longitud, en octetos, de los datos de identificación, incluyendo la cabecera de carga genérica.
- Tipo de Identificador (1 octeto): Valor descriptivo de la información de identidad encontrada en el campo Datos de identificación.
- Identificador de Protocolo (1 octeto): Valor que especifica un identificador de protocolo IP asociado (por ejemplo UDP/TCP). Un valor de cero significa que el campo Identificador de Protocolo debería ser ignorado.
- Puerto (2 octetos): Valor que especifica un puerto asociado. Un valor de cero significa que el campo Puerto debería ser ignorado.
- Datos de Identificación (longitud variable): Valor, indicado por el Tipo de Identificador.

4.6.2.1 Valores de los Tipo de Identificadores

La tabla siguiente lista los valores asignados para el campo Tipo de Identificador encontrados dentro de la Carga de Identificación.

Tipo de Identificador	Valor
RESERVADO	0
ID_IPV4_ADDR (Identificador de Dirección IPv4)	1
ID_FQDN (Identificador de Nombre de Dominio Completamente Cuantificado)	2
ID_USER_FQDN (Identificador de Usuario de Nombre de Dominio Completamente Cuantificado)	3
ID_IPV4_ADDR_SUBNET (Identificador de Dirección de Subred IPv4)	4
ID_IPV6_ADDR (Identificador de Dirección IPv6)	5
ID_IPV6_ADDR_SUBNET (Identificador de Dirección de Subred IPv6)	6
ID_IPV4_ADDR_RANGE (Identificador de Rango de direcciones IPv4)	7
ID_IPV6_ADDR_RANGE (Identificador de Rango de direcciones IPv6)	8
ID_DER_ASN1_DN (Identificador DER ASN.1 de Nombre de distribución X.500)	9
ID_DER_ASN1_GN (Identificador DER ASN.1 de Nombre Generales X.500)	10
ID_KEY_ID (Identificador de Identificación Clave)	11

Para los tipos donde la entidad del identificador tiene una longitud variable, el tamaño de la entidad del identificador es calculado a partir del tamaño en la cabecera de carga de identificación.

Cuando un intercambio IKE es autentificado usando certificados (de cualquier formato), cualquier identificador usado para las decisiones de la política local de entrada DEBERÍA ser incluido en el certificado usado en la autentificación del intercambio.

4.6.2.2 ID_IPV4_ADDR

El tipo ID_IPV4_ADDR (Identificador de Dirección IPv4) especifica una sola dirección IPv4 de cuatro (4) octetos.

4.6.2.3 ID_FQDN

El tipo ID_FQDN (Identificador de Nombre de Dominio Completamente cuantificado (FQDN)) especifica una cadena de caracteres que contiene un nombre de dominio completamente cuantificado. Un ejemplo de un ID_FQDN es, "foo.bar.com". La cadena de caracteres no debería contener ningún terminador.

4.6.2.4 ID_USER_FQDN

El tipo ID_USER_FQDN (Identificador de Usuario de Nombre de Dominio Completamente Cuantificado (FQDN)) especifica una cadena de caracteres que contiene un nombre de dominio completamente cuantificado. Un ejemplo de un ID_USER_FQDN es, "piper@foo.bar.com". La cadena de caracteres no debería contener ningún terminador.

4.6.2.5 ID_IPV4_ADDR_SUBNET

El tipo ID_IPV4_ADDR_SUBNET (Identificador de Dirección de Subred IPv4) especifica un rango de direcciones IPv4, representadas por dos valores de cuatro (4) octetos. El primer valor es una dirección IPv4. El segundo valor es una máscara de red IPv4. Note que unos (1s) en la máscara de red indican que el correspondiente bit en la dirección es fijo, mientras que ceros (0s) indican un bit "comodín".

4.6.2.6 ID_IPV6_ADDR

El tipo ID_IPV6_ADDR (Identificador de Dirección IPv6) especifica una sola dirección IPv6 de dieciséis (16) octetos.

4.6.2.7 ID_IPV6_ADDR_SUBNET

El tipo ID_IPV6_ADDR_SUBNET (Identificador de Dirección de Subred IPv6) especifica un rango de direcciones de IPv6 representados por dos valores de dieciséis (16) octetos. El primer valor es una dirección IPv6. El segundo valor es una máscara de red IPv6. Note que unos (1s) en la máscara de red indican que el correspondiente bit en la dirección es fijo, mientras que ceros (0s) indican un bit "comodín".

4.6.2.8 ID_IPV4_ADDR_RANGE

El tipo ID_IPV4_ADDR_RANGE (Identificador de Rango de direcciones IPv4) especifica un rango de direcciones IPv4, representados por dos valores de cuatro (4) octetos. El primer valor es el principio del rango de direcciones IPv4 (incluyendo este valor) y el segundo valor es el final del rango de valores de direcciones IPv4 (incluyendo este valor). Todas las direcciones que están dentro del rango se consideran dentro de la lista.

4.6.2.9 ID_IPV6_ADDR_RANGE

El tipo ID_IPV6_ADDR_RANGE (Identificador de Rango de direcciones IPv6) especifica un rango de direcciones IPv6, representados por dos valores de dieciséis (16) octetos. El primer valor es el principio del rango de direcciones IPv6 (incluyendo este valor) y el segundo

valor es el final del rango de valores de direcciones IPv6 (incluyendo este valor). Todas las direcciones que están dentro del rango se consideran dentro de la lista.

4.6.2.10 ID_DER_ASN1_DN

El tipo ID_DER_ASN1_DN (Identificador DER ASN.1 de Nombre de distribución X.500) especifica la codificación DER (Distinguished Encoding Rules - Regla de codificación de distribución) binaria del Nombre de distribución ASN.1 X.500 [X.501] de cuyos certificados se están intercambiando para el establecimiento de la SA.

4.6.2.11 ID_DER_ASN1_GN

El tipo ID_DER_ASN1_GN (Identificador DER ASN.1 de Nombre General X.500) especifica la codificación DER (Distinguished Encoding Rules - Regla de codificación de distribución) binaria del Nombre General ASN.1 X.500 [X.509] de cuyos certificados se están intercambiando para el establecimiento de la SA.

4.6.2.12 ID_KEY_ID

El tipo ID_KEY_ID (Identificador de Identificación Clave) especifica una cadena de bit oculta, la cual puede ser usada para enviar la información específica del vendedor necesaria para identificar que clave pre-compartida debería ser usada para autentificar la negociación en modo Agresivo.

4.6.3 Tipos de Mensaje de Notificación IPsec

ISAKMP define dos bloques de códigos de Mensajes de Notificación, uno para los errores y el otro para los mensajes de estado. ISAKMP también asigna una parte de cada bloque para uso privado dentro de un DOI. El DOI de IPsec define los siguientes tipos de mensaje privados para su propio uso.

Mensaje de Notificación - Tipos de Error	Valor
RESERVADO	8192

Mensaje de Notificación - Tipos de Estado	Valor
RESPONDER-LIFETIME (Tiempo de Vida del Respondedor)	24576
REPLAY-STATUS (Estado del Anti-replay)	24577
INITIAL-CONTACT (Contacto-Inicial)	24578

Los Mensajes de Notificación de Estado DEBEN ser enviados bajo la protección de una SA ISAKMP ya sea: como una carga en el último intercambio del Modo Principal; o dentro de un Intercambio

Informativo separado después de completarse el procesamiento del Modo Principal o el del Modo Agresivo; o como una carga dentro de cualquier intercambio de Modo Rápido. Estos mensajes NO DEBEN ser enviados dentro de un intercambio de Modo Agresivo, puesto que el Modo Agresivo no proporciona la protección necesaria para vincular el Mensaje de Notificación de Estado al intercambio.

Nota: Una carga de Notificación está completamente protegida en Modo Rápido solo cuando la carga entera es incluida dentro del resumen (digest) HASH(n). En Modo Principal, la carga de notificación es encriptada, esta no se incluye dentro del resumen (digest) HASH(n). Como resultado, un ataque activo por sustitución sobre el texto cifrado en Modo Principal podría provocar que el tipo de mensaje de notificación de estado esté corrupto. (Esto es así, en general, para el último mensaje de cualquier intercambio en Modo Principal.) Mientras que existe menor riesgo de que el mensaje de notificación corrupto pueda causar que el receptor aborte la negociación entera pensando que el emisor encontró un error fatal.

Nota de Implementación: El protocolo ISAKMP no garantiza la entrega de los mensajes de Notificación de Estado cuando son enviados en un Intercambio Informativo ISAKMP. Para garantizar la recepción de cualquier mensaje, el emisor DEBERÍA incluir una Carga de Notificación en un intercambio de Modo Principal o de Modo Rápido específico el cuál es protegido por un tiempo de retransmisión.

4.6.3.1 RESPONDER-LIFETIME

El mensaje de estado RESPONDER-LIFETIME (Tiempo de Vida del Respondedor) se puede utilizar para comunicar el tiempo de vida de la SA IPsec seleccionado por el respondedor.

Cuando está presente, la Carga de Notificación DEBE tener el siguiente formato:

- Longitud de la Carga: determinado por la longitud de la carga más el tamaño de los datos (variable)
- DOI: determinado por el DOI de IPsec (1)
- Identificador de Protocolo: determinado por el Identificador de Protocolo seleccionado a partir de la SA seleccionada.
- Tamaño del SPI: determinado por los dieciséis (16) (los dos cookies ISAKMP de ocho octetos) o por los cuatro (4) (uno del SPI IPsec).
- Tipo de Mensaje de Notificación: determinado por RESPONDER-LIFETIME (Ver Sección 4.6.3)
- SPI: Determinado por los dos cookies de ISAKMP o por los SPI IPsec entrantes del emisor.

- Datos de Notificación: contiene una lista de atributos ISAKMP con el/los tiempo(s) de vida real de la SA del respondedor.

Nota de Implementación: decir que el campo Datos de Notificación contiene una lista de atributos es equivalente a decir que el campo Datos de Notificación tiene una longitud cero y la Carga de Notificación tiene una lista de atributos asociados.

4.6.3.2 REPLAY-STATUS

El mensaje de estado REPLAY-STATUS (Estado del Anti-replay) se puede utilizar para la confirmación positiva de la elección del respondedor de realizar o no la detección del anti-replay.

Cuando está presente, la Carga de Notificación DEBE tener el siguiente formato:

- Longitud de la Carga: determinado por la longitud de la carga más el tamaño de los datos (4)
- DOI: determinado por el DOI de IPsec (1)
- Identificador de Protocolo: determinado por el Identificador de Protocolo seleccionado a partir de la SA seleccionada.
- Tamaño del SPI: determinado por los dieciséis (16) (los dos cookies ISAKMP de ocho octetos) o por los cuatro (4) (uno del SPI IPsec).
- Tipo de Mensaje de Notificación: determinado por REPLAY-STATUS
- SPI: Determinado por los dos cookies de ISAKMP o por los SPI IPsec entrantes del emisor.
- Datos de Notificación: un valor de 4 octetos:
  0 = detección de anti-replay desactivado
  1 = detección de anti-replay activado

4.6.3.3 INITIAL-CONTACT

El mensaje de estado INITIAL-CONTACT (Contacto-Inicial) se puede utilizar cuando un lado desea informar a la otra parte que esta es la primera SA establecida con el sistema remoto. El receptor de este Mensaje de Notificación puede entonces escoger suprimir alguna de sus SA existentes que tiene para el sistema emisor bajo la suposición de que el sistema del emisor ha reiniciado y ya no tiene acceso a sus SA originales y a su material clave asociado. Cuando se usa, el contenido del campo, Datos de Notificación, DEBERÍA ser nulo (es decir la Longitud de la Carga debería estar determinada por la longitud fija de la Carga de Notificación)

Cuando está presente, la Carga de Notificación DEBE tener el siguiente formato:

- Longitud de la Carga: determinado por la longitud de la carga más el tamaño de los datos (0)
- DOI: determinado por el DOI de IPsec (1)
- Identificador de Protocolo: determinado por el Identificador de Protocolo seleccionado a partir de la SA seleccionada.
- Tamaño del SPI: determinado por los dieciséis (16) octetos (los dos cookies ISAKMP de ocho octetos).
- Tipo de Mensaje de Notificación: determinado por INITIAL-CONTACT
- SPI: Determinado por las dos cookies de ISAKMP.
- Datos de Notificación: <no está incluido>

4.7 Requisitos para el Intercambio de Claves IPsec

El DOI de IPsec no introduce tipos de Intercambio de Claves adicionales.

5. Consideraciones de Seguridad

Este documento entero se aplica al protocolo de Intercambio de Claves en Internet ([IKE]), combinado con ISAKMP ([ISAKMP]) y con Oakley ([OAKLEY]) para proporcionar la obtención del material criptográfico clave de forma segura y autentificada. Discusiones especificas de varios protocolos de seguridad y identificación de transformaciones en este documento pueden ser halladas en documentos relacionados y en referencias de cifrado.

6. Consideraciones de la IANA

Este documento contiene varios números "mágicos" que son mantenidos por la IANA. Esta Sección explica el criterio usado por la IANA para asignar números adicionales en cada una de estas listas. Todos los valores definidos no explícitamente en secciones anteriores están reservados por la IANA.

6.1 Definición de Situación IPsec

La Definición de Situación es una máscara de bit (bitmask) el cual representa el ambiente bajo el cual la propuesta SA IPsec y la negociación es llevada a cabo. Pedidos de asignaciones de nuevas situaciones deben estar acompañados por un RFC el cual describa la interpretación para los bit asociados.

Si el RFC no esta sobre la pila de estándares (es decir, es un RFC informativo o experimental), debe ser revisado explícitamente y aprobado por el IESG (Internet Engineering Steering Group) antes de que el RFC sea publicado y el identificador de transformación sea asignado.

Los dos bit de orden superior están reservados para usarse en forma privada entre sistemas.

6.2 Identificador de Protocolo de Seguridad IPsec

El Identificador de Protocolo de Seguridad es un valor de 8 bit el cual identifica a un conjunto de protocolos de seguridad que es negociado. Pedidos de asignaciones de nuevos identificadores de protocolo de seguridad deben estar acompañados por un RFC el cual describa los requisitos del protocolo de seguridad. [AH] y [ESP] son ejemplos de documentos de protocolos de seguridad.

Si el RFC no esta sobre la pila de estándares (es decir, es un RFC informativo o experimental), debe ser revisado explícitamente y aprobado por el IESG (Internet Engineering Steering Group) antes de que el RFC sea publicado y el identificador de transformación sea asignado.

Los valores de 249 a 255 esta reservados para usarse en forma privada entre sistemas.

6.3 Identificador de Transformación ISAKMP IPsec

El Identificador de Transformación ISAKMP es un valor de 8 bit el cual identifica a un protocolo de intercambio de claves que es usado para la negociación. Pedidos de asignaciones de nuevos identificadores de transformación ISAKMP deben estar acompañados por un RFC el cual describa los requisitos para el protocolo de intercambio de claves. [IKE] es un ejemplo de tal documento.

Si el RFC no esta sobre la pila de estándares (es decir, es un RFC informativo o experimental), debe ser revisado explícitamente y aprobado por el IESG (Internet Engineering Steering Group) antes de que el RFC sea publicado y el identificador de transformación sea asignado.

Los valores de 249 a 255 están reservados para usarse en forma privada entre sistemas.

6.4 Identificador de Transformación AH IPsec

El Identificador de Transformación AH IPsec es un valor de 8 bit el cual identifica a un algoritmo particular usado para proporcionar protección de integridad para AH. Pedidos de asignaciones de nuevos identificadores de transformación AH deben estar acompañados por un RFC el cual describa como usar el algoritmo dentro del marco de AH ([AH]).

Si el RFC no esta sobre la pila de estándares (es decir, es un RFC informativo o experimental), debe ser revisado explícitamente y aprobado por el IESG (Internet Engineering Steering Group) antes de que el RFC sea publicado y el identificador de transformación sea asignado.

Los valores de 249 a 255 están reservados para usarse en forma privada entre sistemas.

6.5 Identificador de Trasformación ESP IPsec

El Identificador de Transformación ESP IPsec es un valor de 8 bit el cual identifica a un algoritmo particular usado para proporcionar protección de confidencialidad para ESP. Pedidos de asignaciones de nuevos identificadores de transformación ESP deben estar acompañados por un RFC el cual describa como usar el algoritmo dentro del marco de ESP ([ESP]).

Si el RFC no esta sobre la pila de estándares (es decir, es un RFC informativo o experimental), debe ser revisado explícitamente y aprobado por el IESG (Internet Engineering Steering Group) antes de que el RFC sea publicado y el identificador de transformación sea asignado.

Los valores de 249 a 255 están reservados para usarse en forma privada entre sistemas.

6.6 Identificador de Trasformación IPCOMP IPsec

El Identificador de Transformación IPCOMP IPsec es un valor de 8 bit el cual identifica a un algoritmo particular usado para proporcionar compresión a nivel IP antes de ESP. Pedidos de asignaciones de nuevos identificadores de transformación IPCOMP deben estar acompañados por un RFC el cual describa como usar el algoritmo dentro del marco de IPCOMP ([IPCOMP]). Además el algoritmo requerido debe ser publicado y debe ser de dominio público.

Si el RFC no esta sobre la pila de estándares (es decir, es un RFC informativo o experimental), debe ser revisado explícitamente y aprobado por el IESG (Internet Engineering Steering Group) antes de que el RFC sea publicado y el identificador de transformación sea asignado.

Los valores de 1 a 47 están reservados para algoritmos para los cuales un RFC ha sido aprobado para publicarse. Los valores de 48 a 63 están reservados para usarse en forma privada entre sistemas. Los valores de 64 a 255 están reservados para futuras ampliaciones.

6.7 Atributos de la Asociación de Seguridad IPsec

Los Atributos de la Asociación de Seguridad IPsec consiste de un tipo de 16 bit y de sus valores asociados. Los atributos SA IPsec son usados para pasar diversos valores entre usuarios ISAKMP. Pedidos de asignaciones de nuevos atributos SA IPsec deben estar acompañados por un Draft de Internet el cual describa la codificación del atributo (Básico/Longitud-Variable) y sus valores válidos. La Sección 4.5 de este documento proporciona un ejemplo de tal descripción. Los valores de 32001 a 32767 esta reservados para usarse en forma privada entre sistemas.

6.8 Identificador de Dominio de Identificación IPsec

El Identificador de Dominio de Identificación IPsec es un valor de 32 bit el cual identifica a un espacio de asignación de nombres (namespace) en el cual existen niveles de Confidencialidad y Integridad y valores de categorías. Pedidos de asignaciones de nuevos identificadores de dominio de identificación se deberían conceder o demandar. No se requiere que lo acompañe documentación, sin embargo se aconsejan Drafts Internet cuando sea apropiado.

Los valores de 0x80000000 a 0xffffffff están reservados para usarse en forma privada entre sistemas.

6.9 Tipo de Identificador IPsec

El Tipo de Identificador IPsec es un valor de 8 bit el cual es usado como un discriminante para interpretar la longitud variable de la Carga de Identificación. Pedidos de asignaciones de nuevos Tipos de Identificador IPsec deben estar acompañados por un RFC el cual describa como usar el tipo de identificador dentro de IPsec.

Si el RFC no esta sobre la pila de estándares (es decir, es un RFC informativo o experimental), debe ser revisado explícitamente y aprobado por el IESG (Internet Engineering Steering Group) antes de que el RFC sea publicado y el identificador de transformación sea asignado.

Los valores de 249 a 255 están reservados para usarse en forma privada entre sistemas.

6.10 Tipos de Mensajes de Notificación IPsec

Los Tipos de Mensajes de Notificación IPsec es un valor de 16 bit tomado del rango de valores reservados por ISAKMP para cada DOI. Hay un rango de mensajes de error (8192 a 16383) y un rango diferente para los mensajes de estado (24576 a 32767). Pedidos de asignaciones

de nuevos Tipos de Mensajes de Notificación deben estar acompañados por un Draft de Internet el cual describa como se usa el tipo de identificador dentro de IPsec.

Los valores de 16001 a 16383 y los valores de 32001 a 32767 están reservados para usarse en forma privada entre sistemas.

7. Cambios en las Versiones

7.1 Cambios a Partir de la Versión N°9

- Se agregaron la referencia explicitas [IPCOMP], [DEFLATE], y [LZS]
- Se permite que RESPONDER-LIFETIME y REPLAY-STATUS sean administrados en un SPI IPsec en añadido al "SPI" ISAKMP.
- Se añadió la exclusión de relleno al texto de la Longitud de Secreto y de la Longitud de Integridad.
- Se añadieron referencias a la Sección 4.5 en la Sección 4.4.4
- Se actualizaron los documentos de referencia.

7.2 Cambios a Partir de la Versión N°8

- Se actualizaron los rangos de Identificadores IPCOMP para reflejar mejor el draft IPCOMP
- Se actualizaron las consideraciones de la IANA por el texto sugerido de Jeff/ Ted's
- Se elimino la referencia al Identificador DES-MAC([DESMAC])
- se corrigió el error en la Sección Notificación; Notificación ISAKMP es un valor de 16 bits.

7.3 Cambios a Partir de la Versión N°7

- Se corrigió el nombre de IPCOMP (Compresión de la Carga IP)
- Se corrigió la referencia a [ESPCBC]
- Se añadió la perdida de Nivel de Secreto y el Nivel de Integridad en la Figura 1
- Se quito la referencia al Identificador para PF_KEY y ARCFOUR
- Se actualizo el texto Básico/Variable para alienarlo con [IKE]
- Se actualizo documentos de referencia y se agregaron punteros hacia [ARCH]
- Se actualizo requerimientos de Notificación; se quitaron referencia dinámicas
- Se agregó la clasificación sobre protección para cargas de Notificación
- Se restablecido RESERVADO para el espacio de asignación de nombres (namespace) del identificador de transformación ESP; motivado por ESP_NULL

- Se agregó requerimientos para el soporte de ESP_NULL y referencias [ESPNULL]
- Se agregó la aclaración sobre Autentificación de Algoritmo usado en AH/ESP
- Se agregó restricción de usos conflictivos en combinaciones AH/Autentificación

7.4 Cambios a Partir de la Versión N°6

Los siguientes cambios fueron realizados en relación con el DOI de IPsec Versión N°6:

- Se agrego la Sección Consideraciones de la IANA
- Se debió mover los números de la IANA a la Sección Consideraciones de la IANA
- Se agrego la prohibición sobre el envió (V) codificado (B) para el atributo
- Se agrego la prohibición sobre el atributo Longitud de la Clave para los cifrados de longitud fija (por ejemplo DES)
- Se reemplazaron las referencias a ISAKMP/Oakley con IKE
- Se reemplazo ESP_ARCFOUR por ESP_RC4
- Se actualizo la Sección Consideraciones de Seguridad
- Se actualizaron los documentos de referencia

7.5 Cambios a Partir de la Versión N°5

Los siguientes cambios fueron realizados en relación con el DOI de IPsec Versión N°5:

- Se cambio el tamaño del SPI en el texto Notificación del Tiempo de Vida.
- Se cambio REPLAY-ENABLED por REPLAY-STATUS
- Se movió la definición de la carga RESPONDER-LIFETIME de la Sección 4.5.4 hacia la Sección 4.6.3.1
- Se agrego el diseño de la carga explicita de la 4.6.3.3
- Se agrego Notas de Implementación en la Sección 4.6.3
- Se cambio el texto AH_SHA de requerido SHA-1 además de MD5
- Se actualizaron los documentos de referencia

7.6 Cambios a Partir de la Versión N°4

Los siguientes cambios fueron realizados en relación con el DOI de IPsec Versión N°4:

- Se movió la compatibilidad del método de autentificación AH KPDK de identificador de transformación AH hacia el identificador de Algoritmo de Autentificación

- Se agrego el tipo mensaje de notificación REPLAY-ENABLED por la Arquitectura
- Se agrego el tipo mensaje de notificación INITIAL-CONTACT por la lista
- Se agrego el texto protección asegurada para el mensaje Notificación de Estado
- Se agrego la clasificación tiempo de vida para la Sección descomposición del atributo
- Se agrego la aclaración de que la notificación del tiempo de vida es opcional
- Se quito la lista de Descripción de Grupos privados (nueva posición en [IKE])
- Se reemplazo terminología con punteros hacia el RFC-2119
- Se actualizo referencias HMAC MD5 y identificador SHA-1
- Se actualizo la Sección 1 (Resumen)
- Se actualizo la Sección 4.4 (Números Asignados a IPsec)
- Se agrego restricciones para los valores de identificadores puerto/protocolo de la Fase 1

7.7 Cambios a Partir de la Versión N°3 hasta la versión N°4

Los siguientes cambios fueron realizados en relación con el DOI de IPsec Versión N°3, es decir fue enviado a la lista de IPsec antes del IETF de Munich:

- Se añadió el identificador de transformación ESP para NULL y ARCFOUR
- Se renombro el Algoritmo HMAC para acomodarlo al Algoritmo de Autentificación DES-MAC y a la autentificación/integridad opcional de ESP
- Se agrego el identificador de algoritmo DES-MAC a AH y ESP
- Se elimino la definición del identificador KEY_MANUAL y KEY_KDC
- Se agrego que la duración del tiempo de vida DEBE estar seguida del atributo tipo de vida para la definición del atributo Tipo de Vida de la SA y Tiempo de Vida de la SA
- Se agrego la notificación del tiempo de vida y el tipo de mensaje DOI de IPsec
- Se agrego autentificación opcional y restricciones de confidencialidad para la definición del atributo del Algoritmo MAC
- Se corrigió el ejemplo del atributo descomponer (uso obsoleto del atributo)
- Se corrigieron varios documentos de referencias a Draft Internet
- Se añadió ID_KEY_ID por la lista de discusión IPsec(18-Mar-97)
- Se quito la Descripción de Grupos para PFS (Perfect Forward Secrecy) QM (Modo Rápido - Quick Mode), (DEBE estar en [IKE])

Agradecimientos

Este documento es obtenido, en parte, de trabajos previos de Douglas Maughan, Mark Schertler, Mark Schneider, Jeff Turner, Dan Harkins, y Dave Carrel. Matt Thomas, Roy Pereira, Greg Carter, y Ran Atkinson tambien contribuyeron con sugerencias y, en muchos casos, con textos.

Referencias

[AH] Kent, S., and R. Atkinson, "IP Authentication Header", RFC 2402, November 1998.

[ARCH] Kent, S., and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[DEFLATE] Pereira, R., "IP Payload Compression Using DEFLATE", RFC 2394, August 1998.

[ESP] Kent, S., and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.

[ESPCBC] Pereira, R., and R. Adams, "The ESP CBC-Mode Cipher Algorithms", RFC 2451, November 1998.

[ESPNULL] Glenn, R., and S. Kent, "The NULL Encryption Algorithm and Its Use With IPsec", RFC 2410, November 1998.

[DES] Madson, C., and N. Doraswamy, "The ESP DES-CBC Cipher Algorithm With Explicit IV", RFC 2405, November 1998.

[HMACMD5] Madson, C., and R. Glenn, "The Use of HMAC-MD5 within ESP and AH", RFC 2403, November 1998.

[HMACSHA] Madson, C., and R. Glenn, "The Use of HMAC-SHA-1-96 within ESP and AH", RFC 2404, November 1998.

[IKE] Harkins, D., and D. Carrel, D., "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[IPCOMP] Shacham, A., Monsour, R., Pereira, R., and M. Thomas, "IP Payload Compression Protocol (IPComp)", RFC 2393, August 1998.

[ISAKMP] Maughan, D., Schertler, M., Schneider, M., and J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)", RFC 2408, November 1998.

[LZS] Friend, R., and R. Monsour, "IP Payload Compression Using LZS", RFC 2395, August 1998.

[OAKLEY] Orman, H., "The OAKLEY Key Determination Protocol", RFC 2412, November 1998.

[X.501] ISO/IEC 9594-2, "Information Technology - Open Systems Interconnection - The Directory: Models", CCITT/ITU Recommendation X.501, 1993.

[X.509] ISO/IEC 9594-8, "Information Technology - Open Systems Interconnection - The Directory: Authentication Framework", CCITT/ITU Recommendation X.509, 1993.

Author's Address

Derrell Piper
Network Alchemy
1521.5 Pacific Ave
Santa Cruz, California, 95060
United States of America

Phone: +1 408 460-3822
EMail: ddp@network-alchemy.com

Declaración de Copyright Completa

Notas del Traductor

Los Términos que aparecen entre "[]" que no sean referencias reflejan la palabra/s en inglés de las palabra/s que se encuentran (en español) a la izquierda, debido a que NO ESTOY SEGURO de que sea la correcta traducción del término o simplemente para que no se pierda el VERDADERO sentido del texto.

Esta presente traducción fue realizada por Hugo Adrian Francisconi para mi tarjado de tesis de "Ingeniero en Electrónico" en la Facultad U.T.N. (Universidad Nacional Tecnología) Regional Mendoza - Argentina. Si le interesa IPsec y quieres saber más podes bajarte mi trabajo de tesis, "IPsec en Ambientes IPv4 e IPv6" de http://codarec6.frm.utn.edu.ar, para el cual traduje varios RFCs al español relacionados con IPsec. Cualquier sugerencia debate o comentario sobre este presente tema o traducción será bien recibida en adrianfrancisconi@yahoo.com.ar

Se a realizado el máximo esfuerzo para hacer de esta traducción sea tan completa y precisa como sea posible, pero no se ofrece ninguna garantía implícita de adecuación a un fin en particular. La información se suministra "tal como está". El traductor no será responsable ante cualquier persona o entidad con respecto a cualquier pérdida o daño que pudiera resultar emergente de la información contenida en está traducción.

Derechos de Copyright Sobre Esta Traducción

Datos del Traductor

Nombre y Apellido del Traductor: Hugo Adrian Francisconi
Domicilio: Carril Godoy Cruz 2801, Villa Nueva-Guay Mallen-Mendoza-Argentina
Código Postal: 5500
Tel: 054-0261-4455427
E-mail: adrianfrancisconi@yahoo.com.ar