Recomendaciones de Seguridad para VPN IPSec

1. INTRODUCCIÓN A LAS VPN

Las *Virtual Private Networks (*VPNs) son una serie de tecnologías que proporcionan una conexión segura entre distintas redes de una misma organización o entre usuarios remotos que necesitan acceder a los recursos de ésta, utilizando como soporte de comunicaciones cualquier red del dominio público, como Internet. A través de las VPNs, la organización puede extender su red interna al mismo tiempo que protege sus recursos de las redes públicas que soportan la conexión.

Las principales ventajas de implementar VPNs son las siguientes:

a) Se garantiza la seguridad en los siguientes aspectos:
   - **Confidencialidad de los datos**, al emplear mecanismos de cifrado.
   - **Integridad de los datos**, al emplear mecanismos de *hashing*.
   - **Autenticación extremo a extremo**.
   - **Aislamiento de flujos de datos.**
   - **Aplicación de políticas de seguridad corporativas**, al adquirir el cliente remoto la condición de miembro de la red interna de la organización. De este modo podrán aplicársele todas las directrices y políticas de seguridad de la organización.

b) El uso de una infraestructura pública como Internet supone un ahorro de costes frente a otros mecanismos de implementación de comunicaciones seguras, como por ejemplo enlaces privados dedicados o líneas dedicadas.

c) Posibilidad de escalabilidad dentro de una red.

Todo ello, unido al hecho de que cada vez es más común que ciertos dispositivos de red como cortafuegos o enrutadores implementen esta capacidad, hace que la utilización de VPNs esté cada vez más extendida.

No obstante, la utilización de VPNs también lleva añadido un riesgo dado que permitimos un acceso directo a nuestra red corporativa, abriendo una vía de acceso externo en el perímetro de seguridad. En ocasiones, malas implementaciones, configuraciones o la utilización de protocolos o algoritmos poco adecuados o que no implementan la fortaleza criptológica necesaria pueden traer como consecuencia la exposición de datos sensibles.

Existen distintos tipos de VPN que se establecen a nivel de enlace, red o transporte. No obstante, en este documento nos centraremos en las recomendaciones relativas a las VPN IPSec, que operan íntegramente a nivel de red.

2. SELECCIÓN DE DISPOSITIVOS O HERRAMIENTAS: PRODUCTOS CUALIFICADOS Y PRODUCTOS APROBADOS

Recomendación 1:
Para aquellos **sistemas afectados por el Esquema Nacional de Seguridad (ENS)**, deberán utilizarse productos recogidos en el apartado de **Productos Cualificados** en las familias Redes Privadas Virtuales o Cifradores IP **dentro del Catálogo de Productos de Seguridad TIC (CPSTIC).** Deberá tenerse en cuenta la categoría del ENS para el cual está cualificado el producto y su guía de configuración aprobada.

Para aquellos **sistemas que manejan información clasificada** deberán utilizarse productos recogidos en el apartado de **Productos Aprobados** en las familias Redes Privadas Virtuales o Cifradores IP **dentro del Catálogo de Productos de Seguridad TIC (CPSTIC).** Deberá tenerse en cuenta el nivel de clasificación para el cual está aprobado el producto y su Procedimiento de empleo.

3. IPSEC (RFC 4301)

IPSec es un estándar abierto para comunicaciones VPN que opera a nivel de red, proporciona seguridad a la comunicación y es transparente para el nivel de aplicación. Típicamente es utilizado en dos configuraciones: de acceso remoto y *site to site*.

Además, puede trabajar en dos modos: modo transporte y modo túnel, como veremos en sucesivos apartados.

3.1. VPN de acceso remoto

Esta configuración es típicamente utilizada por los usuarios remotos de una organización que establecen túneles IPSec para conectarse a la red local de ésta. La conexión se realiza desde un dispositivo portátil/móvil/ordenador de sobremesa en el que se encuentra instalada una aplicación de cliente IPSec, que establece la conexión con un dispositivo VPN (típicamente un cortafuegos o un enrutador).

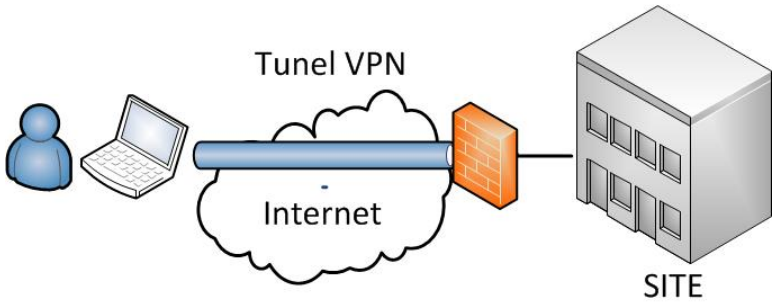

Figura 1 Caso de uso 1: VPN Acceso remoto

3.2. VPN site to site

Esta configuración es típicamente utilizada para interconectar dos sedes de una organización. En este caso, dos dispositivos VPN establecen un túnel IPSec por el que se comunican de forma segura.

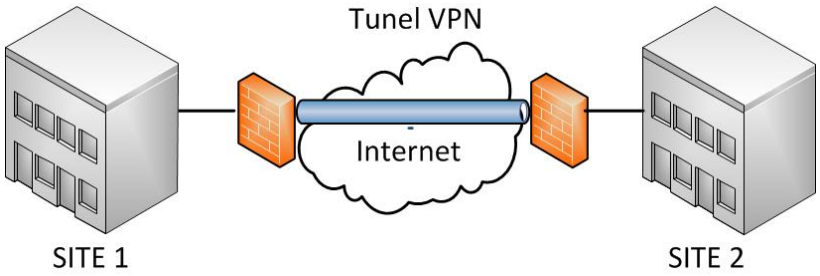

Figura 2 Caso de uso 2: VPN Site to Site

4. CONSTRUCCIÓN DEL PAQUETE IPSEC: MODO TRANSPORTE Y MODO TÚNEL

4.1. Modo transporte

Para la construcción del paquete IPSec en modo transporte sencillamente se añade una cabecera IPSec al paquete IP, pero sigue manteniéndose la cabecera original, por lo que no se oculta dicha información.

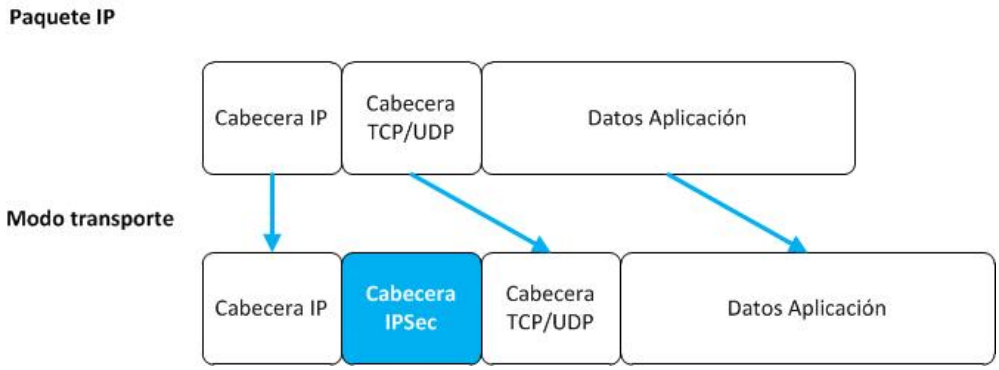

Figura 3 Construcción del paquete IPSec en modo transporte

4.2. Modo túnel

En el modo túnel, todo el paquete IP original se convierte en *payload* de un nuevo paquete IP de mayor longitud. En este caso se añade una nueva cabecera IP, lo que permite ocultar la información de red de ambas entidades.

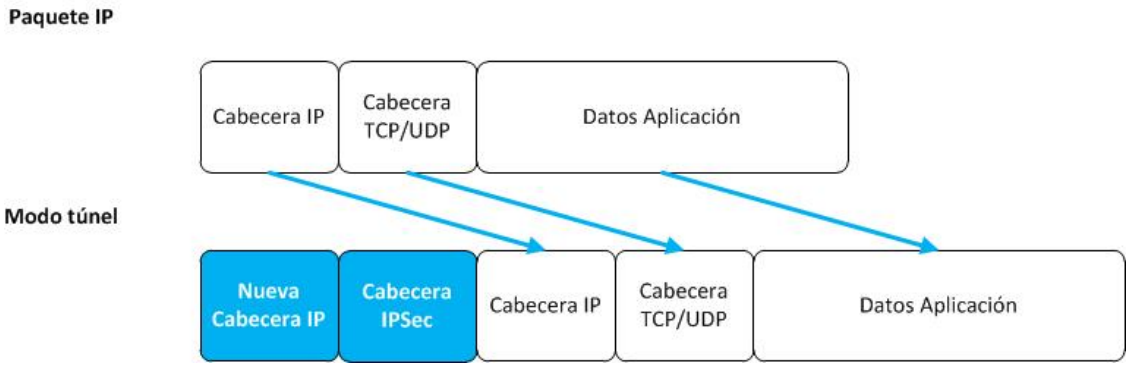

Figura 4 Construcción del paquete IPSec en modo túnel

Recomendación 2:
El modo túnel ofrece una mayor seguridad que el modo transporte. Por ello, **siempre que sea posible se trabajará en esta configuración**. La elección del modo transporte solamente está justificada en el caso de que el tamaño del paquete sea un problema debido a las restricciones impuestas por la red.

Una implementación de equipo Final (*End Point)* debe soportar ambos modos, mientras que una implementación de Pasarela (*Gateway)* debe implementar modo túnel y podrá implementar modo transporte. El uso de este último solo se justifica en el caso de que actúe como *End Point* o provea seguridad entre dos nodos intermedios en un sistema.

5. COMPONENTES IPSEC

IPSec está formado por un conjunto de protocolos, que se enumeran a continuación:

1. *Internet Key Exchange* (IKE). Es el protocolo utilizado para la gestión de las asociaciones de seguridad (SA) y el intercambio de clave.
2. *Authentication Headers* (AH): Es el protocolo que se utiliza para garantizar la integridad de los datos y la Autenticidad del origen, además de protección contra ataques de repetición.
3. *Encapsulation Security Payload*. (ESP). Es el protocolo utilizado principalmente para garantizar la confidencialidad de la información.

Dada su complejidad y la gran variedad de opciones, con frecuencia IPSec no se implementa de manera adecuada y las configuraciones seleccionadas, incluido las que se consideran por defecto en los dispositivos, no son siempre apropiadas, lo que conduce a un nivel de seguridad menor que el deseado.

5.1. Asociaciones de seguridad (SA)

IPSec define la conexión entre dos extremos mediante el término “Asociación de Seguridad” (SA, *Security Association*). Cada SA contiene los detalles de la conexión, el modo de funcionamiento (túnel o transporte), el protocolo empleado (AH, ESP o ambos), información de los algoritmos criptográficos empleados y un índice (SPI, *Security Parameter Index*) que identifica la conexión de forma unívoca. Tienen la particularidad de que se definen en una sola dirección, por ello, para una comunicación bidireccional es necesario establecer dos asociaciones de seguridad, cada una de las cuales tendrá asociados unos parámetros específicos.

Un extremo IPSec puede tener múltiples SA con el mismo o distintos extremos, cada una de ellas con distinto SPI. Típicamente se emplean políticas de seguridad diferentes en base a la IP destino.

Las conexiones IPSec podrán soportar gestión de SA y claves criptográficas manual y automática. Las técnicas manuales son prácticas en entornos pequeños, en los que existe un único administrador de seguridad, y en entornos estáticos. En los casos restantes este tipo de técnicas suele presentar problemas de escalabilidad.

Recomendación 3:
Salvo casos muy específicos, de entornos pequeños con un único administrador de seguridad, **no se recomienda la gestión manual de las SA y del material criptográfico**. Deberá realizarse utilizando IKE.

5.2. IKE

El protocolo de establecimiento y mantenimiento de las SA utilizado por IPSec se denomina IKE. Una de las funciones principales de IKE es el realizar el acuerdo de claves para las SAs.

IKE implementa autenticación mutua entre ambos extremos y establece una asociación de seguridad denominada IKE SA, mediante la cual realiza un intercambio secreto de claves *Diffie-Hellman*, con objeto de establecer una clave de sesión compartida que será utilizada para generar las SA de los protocolos ESP y AH.

Actualmente existen dos versiones del protocolo IKE: IKEv1 e IKEv2, la segunda versión más actual que la primera. En este documento no se incluirán recomendaciones relativas a IKEv1, y nos centraremos en IKEv2, dado que la primera se trata de una versión casi en desuso, por la complejidad del protocolo y del mayor ancho de banda que requiere para el intercambio de claves.

Recomendación 4:
Siempre que sea posible, **deberá utilizarse IKEv2 en lugar de IKEv1**.

5.2.1 IKEv2: intercambios

Como ya hemos indicado en el punto anterior, el protocolo para la gestión de claves utilizado por IPSec deberá ser IKEv2. Este protocolo está definido en la norma RFC 7296 (una revisión de las anteriores RFC 5996 y RFC 4306).

Todas las comunicaciones de IKE consisten en pares de mensajes petición/respuesta (intercambios):

- El primer intercambio IKE_SA_INIT negocia algoritmos criptográficos, intercambia *nonces* (números de un solo uso) y realiza un intercambio *Diffie-Hellman* (DH) a partir del cual se genera un secreto compartido. Todos los mensajes a partir de este intercambio estarán criptográficamente protegidos utilizando los algoritmos y claves negociados.
- El segundo par de mensajes (IKE_AUTH) autentica los mensajes previos, intercambia identidades y certificados y establece la primera SA derivada (*Child SA)*. La confidencialidad y la integridad de este segundo par de mensajes está protegida con el material acordado en el primer intercambio.
- Existen otros tipos de intercambios como el CREATE_CHILD_SA o el INFORMATIONAL, que son opcionales y que, en todo caso, irán siempre protegidos criptográficamente. CREATE_CHILD_SA se utiliza para crear las nuevas Child SA y para renegociar la clave de la IKE_SA y las Child SA.

La autenticación de los extremos en IKE_AUTH puede realizarse de dos maneras: mediante claves pre-compartidas (*pre-shared-keys* o PSK) o mediante mecanismos de criptografía asimétrica (certificados digitales).

Recomendación 5:
Para la **autenticación de extremos en IKEv2 se recomienda utilizar mecanismos de criptografía asimétrica, especialmente aquellas basadas en uso de PKI**, en lugar de claves pre-compartidas (PSK), por dos motivos principales: cualquier parte que sepa la PSK podría autenticarse y conectarse a la VPN, y suelen ser vulnerables a ataques de diccionario.
Únicamente deberían utilizarse cuando sea posible asegurar que han sido generadas con la entropía suficiente para aportar la fortaleza deseada (Ej.: para sistemas del ENS categoría Alta se exigen 128 bits) y es posible renovarlas en un período inferior a su "cripto período".
También existe una **opción de no autenticación**, aunque **no debe utilizarse**.

El protocolo IKE habitualmente escucha y recibe mensajes en el puerto UDP 500, aunque también pueden recibirse en el 4500 con un formato ligeramente diferente.

5.2.2 IKEv2: Generación de claves

Para la generación de todo el material criptográfico que se utilizará para las IKE SA y las IPSec SA se utilizará la derivación de claves. Para ello, se intercambiarán claves efímeras mediante un algoritmo Diffie Hellman y se calculará mediante una función pseudoaleatoria (PRF).

Recomendación 6:
Para la generación de claves deberán emplearse Grupos Diffie-Hellman que cuenten con la fortaleza necesaria. En ningún caso se utilizarán grupos con una fortaleza inferior a 112 bits, es decir, grupos con longitud de módulo de al menos 2048 bits o grupos definidos por curvas elípticas sobre campos primos mayores o iguales a 224 bits.

Recomendación 7:
Para la generación de valores aleatorios se recomienda el uso de funciones pseudoaleatorias basadas en HMAC-SHA2 o en algoritmos de cifrado AES128.

Actualmente se encuentran definidos 32 grupos Diffie-Hellman, aunque no todos ellos están disponibles en las implementaciones de IKE. La siguiente tabla muestra un listado de los grupos más utilizados para establecer VPN en las implementaciones actuales:

Grupo	Descripción	Fortaleza	Uso permitido
1	MODP[1] 768 bit	<112	No permitido
2	MODP 1024 bit	<112	No permitido
5	MODP 1536 bit	<112	No permitido
7	EC2N[2] sobre GF[2^163]	<112	No permitido
14	MODP 2048 bit	112	Hasta 2022
15	MODP 3072 bits	128	Posterior a 2025

[1] MODP: Grupo de exponenciación módulo P, siendo P primo.
[2] EC2N: Grupo basado en curvas elípticas sobre campos finitos.

Grupo	Descripción	Fortaleza	Uso permitido
19	256-bit random EC[3]	128	Posterior a 2025
20	384-bit random EC[4]	192	Posterior a 2025
21	512-bit random EC[5]	256	Posterior a 2025
24	MODP 2048 con subgrupo de orden primo 256 bit	112	Hasta 2022
28	Brainpool Elliptic Curve P256r1	128	Posterior a 2025
29	Brainpool Elliptic Curve P384r1	192	Posterior a 2025
30	Brainpool Elliptic Curve P512r1	256	Posterior a 2025

Recomendación 8:
En caso de seleccionar un grupo basado en curvas elípticas, siempre que sea posible, se recomienda el uso de curvas Brainpool (28, 29 o 30).

5.2.3 IKEv2: Tiempo de vida de las SA

Para cada asociación de seguridad se podrá negociar un tiempo de vida que podrá estar basado en tiempo o en el volumen de datos transmitido, aunque se dará siempre prioridad a los criterios basados en tiempo. En IKEv2 no se podrá renegociar este tiempo una vez se haya establecido. Además, cada extremo de la SA podrá tener un tiempo de vida diferente estipulado para dicha SA, en este caso el extremo que haya configurado ese tiempo de vida menor será el que solicite la renovación o cierre de la SA.

Recomendación 9:
El tiempo de vida máximo recomendado para cada SA dependerá de las exigencias de cada aplicación y será inversamente proporcional al grado de clasificación o sensibilidad de la información que va a transmitir. A mayor frecuencia de renovación de claves mayor seguridad, aunque es necesario tener en cuenta posibles limitaciones impuestas por el tamaño de la red o el ancho de banda con el que se trabaja.
El tiempo de vida de las Child SA no deberá ser mayor que el de las IKE SA y, en general, se recomiendan valores inferiores a 4 horas para las Child SA e inferiores a 24 h para las IKE SA.

5.2.4 IKEv2: Perfect Forward Secrecy (PFS)

La opción de ***Perfect Forward Secrecy*** impide que se descifre el contenido de la comunicación aunque se comprometan las claves establecidas para las asociaciones de seguridad. Por ello, a pesar de que supone incrementos en coste computacional, es altamente recomendable.

[3] RFC5903 basada en las curvas elípticas definidas por el NIST
[4] RFC5903 basada en las curvas elípticas definidas por el NIST
[5] RFC5903 basada en las curvas elípticas definidas por el NIST

En el primer intercambio de IKE se generan las claves para las asociaciones de seguridad IKE y Child. Si se negocian más Child SA partiendo de las IKE SA existentes, el protocolo da la opción de realizar un nuevo intercambio *Diffie-Hellman*, lo que permite que se calculen nuevas claves para sesión. De esta forma, aunque se comprometan las claves intercambiadas inicialmente, no es posible comprometer las claves posteriores.

Recomendación 10:
Deberá activarse el PFS en IKEv2. Además se forzará la renovación de claves cada cierto tiempo o cada cierto volumen de datos.

5.3. Servicios de seguridad: AH y ESP

Los servicios de seguridad que provee IPSec, están basados en dos protocolos diferentes, que son el núcleo de la tecnología IPSec.

1. AH: *Authentication Header*, estandarizado en la RFC 4302.
2. ESP: *Encapsulating Security Payload*, estandarizado en la RFC 4303.

Ambos se utilizan independientemente, o uno u otro y en raras ocasiones se utilizan ambos a la vez.

5.3.1 Authentication Header (AH)

Proporciona identificación del origen así como integridad de datos, protección contra *spoofing* y ataques de repetición. No cifra el contenido del paquete y por lo tanto no aporta protección de la confidencialidad. Los mecanismos de autenticación se aplican a todo el paquete, incluidos los campos cambiantes (aquellos que cambian al pasar entre los diferentes enrutadores a medida que el paquete se transporta a su destino), como las direcciones IP, por lo que este protocolo suele presentar problemas de funcionamiento en entornos donde se utilice NAT (*Network Address Translation*).

AH suele considerarse un protocolo obsoleto y su implementación es opcional. La siguiente figura muestra la estructura del paquete cuando se utiliza este protocolo.

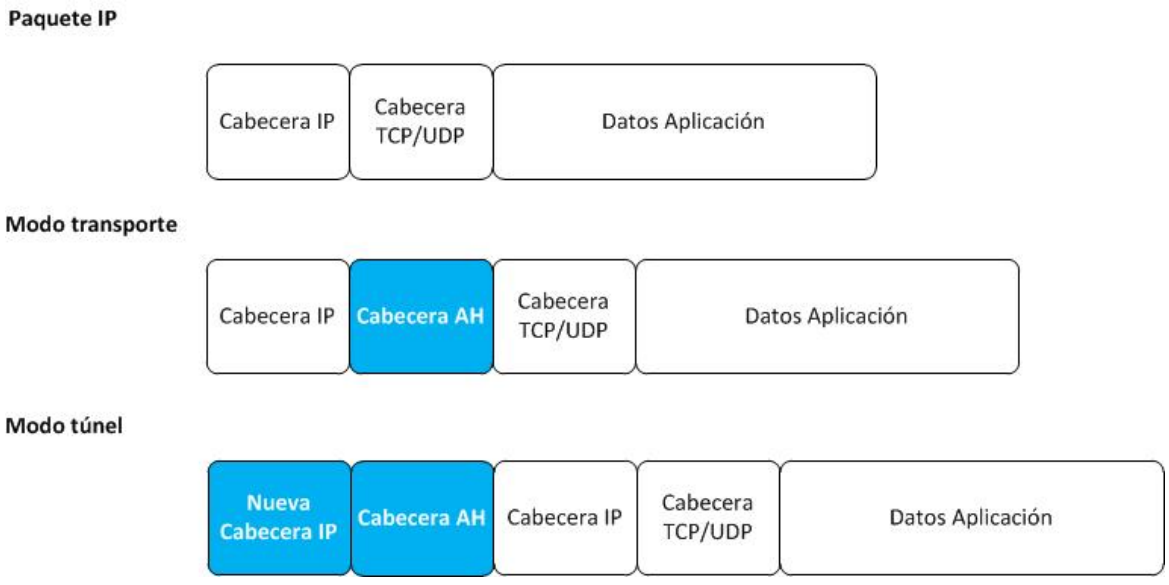

Figura 5 Construcción de paquete AH

Recomendación 11:
AH (*Autentication Header*) es un protocolo opcional cuyo uso **no se recomienda**. En caso de que no sea necesaria protección de la confidencialidad se recomienda utilizar ESP con la opción de no cifrado.

5.3.2 Encapsulating Security Payload (ESP)

Este protocolo proporciona protección de la confidencialidad y la integridad de los paquetes IP y, utilizado junto con IKE, autenticación extremo a extremo y no repudio. También protege contra ataques de repetición.

A diferencia de lo que ocurría con AH, en el que se autenticaba todo el paquete, en ESP solamente está autenticado el *payload*, por lo que cuando se trabaja en modo transporte no se autentica la cabecera IP del paquete.

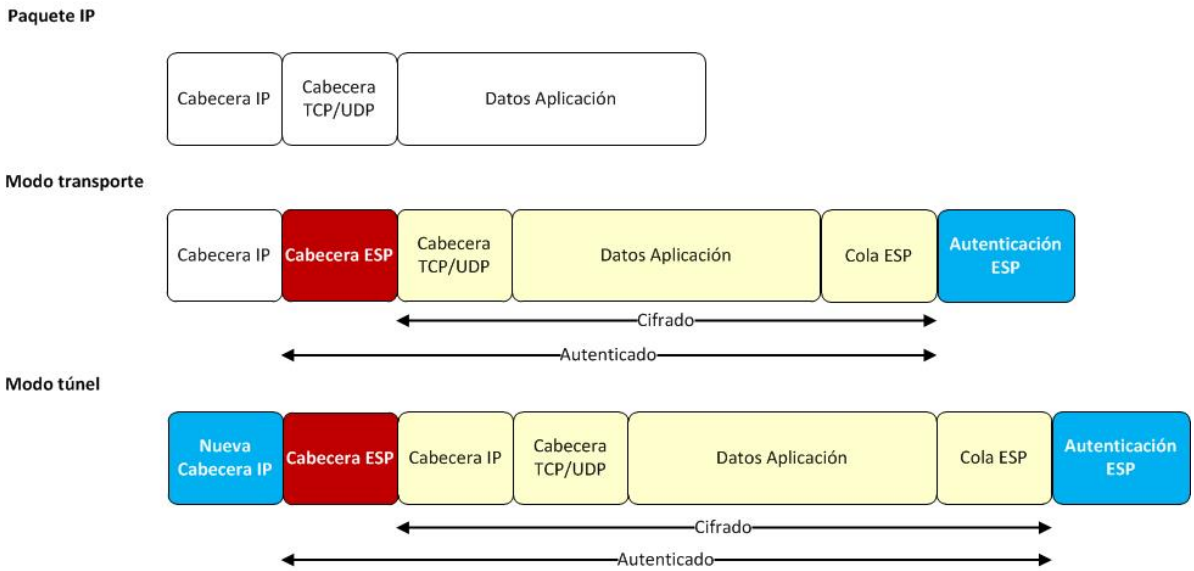

Figura 6 Construcción de paquete ESP

Recomendación 12:
Se recomienda el uso de ESP frente a AH. Se puede configurar sin cifrado o sin control de integridad, aunque no se recomienda.

5.3.3 Encapsulating Security Payload: cifrado y protección de integridad

Como ya se ha indicado anteriormente, ESP puede ser utilizado para ofrecer protección de confidencialidad y de integridad o únicamente protección de integridad.

ESP utiliza un algoritmo de cifrado simétrico para proporcionar confidencialidad. Estos algoritmos dividen los datos en bloques de 128 bits y los cifran. Para aportar protección de la integridad, el primer paso es crear un MAC (*Message Authentication Code*) del mensaje cifrado, utilizando un algoritmo MAC y una clave secreta compartida entre los dos *end points*. El MAC se añade al paquete y el paquete se envía. En la mayor parte de los casos, IPSec utiliza un código de autenticación protegido por clave (*keyed-hash message authentication code* , HMAC) para la

protección de integridad (Ej.: HMAC-SHA-256). Otro algoritmo no basado en HMAC comúnmente utilizado es AES-XCBC-MAC-96.

No obstante, la utilización de algoritmos de cifrado y protección de integridad diferentes requiere dos procesos criptográficos que utilizan diferentes claves. En la práctica, existen algoritmos que combinan ambos procesos y cuyo uso incrementa sensiblemente las prestaciones.

Recomendación 13:
Los algoritmos de cifrado simétrico más comúnmente utilizados en ESP son AES-GCM y AES-CBC o AES-CTR con HMAC-SHA. No obstante, siempre que sea posible se recomienda la utilización de AES-GCM (o de algún otro modo de cifra simétrica autenticado *"Encrypt-Then-MAC"*), dado que ofrece protección de confidencialidad y de integridad en un único proceso.

5.4. NAT + IPSEC = NAT-T

Los elementos con capacidad de traducción de direcciones o NAT (*Network Access Translation*) no son compatibles con los protocolos IPSec por defecto, ya que NAT realiza modificaciones en las cabeceras de los paquetes IP, y los protocolos IPSec protegen los paquetes IP (incluidas las cabeceras) frente a modificaciones. Los motivos fundamentales son:

- El uso del protocolo AH, como hemos visto, autentica todo el paquete, incluidas las cabeceras.
- Los *checksum* calculados en las cabeceras TCP y UDP dependen de las direcciones IP origen y destino. Los protocolos IPSec verifican el *checksum*, por lo que, si se han modificado las direcciones, el paquete sería descartado. Esto no aplicaría si se usa ESP en modo túnel o no se utiliza el checksum en UDP.
- IKE negocia los detalles de la comunicación IPSec, incluyendo las direcciones, puertos a emplear, etc. Si se modifican estos valores negociados se invalidaría el paquete.

NAT-T, conocido como NAT Transversal (RFC- 3947), es un estándar diseñado para solucionar la problemática existente entre IPSec y los entornos de NAT. Este estándar se basa en encapsular los paquetes IPSec en paquetes UDP, de forma que las modificaciones realizadas por los entornos de NAT lo hagan sobre direcciones existentes en las cabeceras del paquete exterior UDP.

NAT-T emplea por defecto el puerto 4500 para la encapsulación en paquetes UDP, algo que deberá tenerse en cuenta en la configuración de los firewall.

Recomendación 14:
Si es necesario emplear NAT en las comunicaciones, deberá activarse la opción de NAT Transversal.

6. CRIPTOLOGÍA

Al margen de las consideraciones genéricas establecidas anteriormente, es necesario tener en cuenta las siguientes consideraciones aplicables dentro del contexto nacional.

Recomendación 15:
Todas las VPN que se establezcan en sistemas afectados por el ENS deberán configurarse de tal forma que solamente hagan uso de los algoritmos autorizados para el ENS. Estos algoritmos están descritos en la CCN-STIC-807. Además, también deberán utilizarse los mecanismos y protocolos descritos en la citada guía.

Todos los productos con capacidad de establecer VPN que vayan a ser utilizados en sistemas clasificados deberán haber pasado una evaluación criptológica en la que se comprobará la fortaleza y correcta implementación los mecanismos y algoritmos utilizados, de acuerdo a lo establecido de la CCN-STIC-130.

7. RESUMEN

1) Para aquellos **sistemas afectados por el Esquema Nacional de Seguridad (ENS)**, deberán utilizarse productos recogidos en el apartado de **Productos Cualificados** en las familias Redes Privadas Virtuales o Cifradores IP **dentro del Catálogo de Productos de Seguridad TIC (CPSTIC).** Deberá tenerse en cuenta la categoría del ENS para el cual está cualificado el producto y su guía de configuración aprobada.
   Para aquellos **sistemas que manejan información clasificada** deberán utilizarse productos recogidos en el apartado de **Productos Aprobados** en las familias Redes Privadas Virtuales o Cifradores IP **dentro del Catálogo de Productos de Seguridad TIC (CPSTIC).** Deberá tenerse en cuenta el nivel de clasificación para el cual está aprobado el producto y su Procedimiento de empleo.
2) El modo túnel ofrece una mayor seguridad que el modo transporte. Por ello, **siempre que sea posible se trabajará en esta configuración**. La elección del modo transporte solamente está justificada en el caso de que el tamaño del paquete sea un problema debido a las restricciones impuestas por la red.
3) Salvo casos muy específicos, de entornos pequeños con un único administrador de seguridad, **no se recomienda la gestión manual de las SA y del material criptográfico**. Deberá realizarse utilizando IKE.
4) Siempre que sea posible, **deberá utilizarse IKEv2 en lugar de IKEv1**.
5) Para la **autenticación de extremos en IKEv2 se recomienda utilizar mecanismos de criptografía asimétrica, especialmente aquellas basadas en uso de PKI**, en lugar de claves pre-compartidas (PSK), por dos motivos principales: cualquier parte que sepa la PSK podría autenticarse y conectarse a la VPN, y suelen ser vulnerables a ataques de diccionario.
   Únicamente deberían utilizarse cuando sea posible asegurar que han sido generadas con la entropía suficiente para aportar la fortaleza deseada (Ej.: para sistemas del ENS categoría Alta se exigen 128 bits) y es posible renovarlas en un período inferior a su "cripto período".
   También existe una **opción de no autenticación**, aunque **no debe utilizarse**.
6) Para la generación de claves deberán emplearse Grupos Diffie-Hellman que cuenten con la fortaleza necesaria, ver 7. En ningún caso se utilizarán grupos con una fortaleza inferior a 112 bits, es decir, grupos con longitud de módulo de al menos 2048 bits o grupos definidos por curvas elípticas sobre campos primos mayores o iguales a 224 bits.

7) Para la generación de valores aleatorios se recomienda el uso de funciones pseudoaleatorias basadas en HMAC-SHA2 o en algoritmos de cifrado AES128.
8) En caso de seleccionar un grupo basado en curvas elípticas, siempre que sea posible, se recomienda el uso de curvas Brainpool (28, 29 o 30).
9) El tiempo de vida máximo recomendado para cada SA dependerá de las exigencias de cada aplicación y será inversamente proporcional al grado de clasificación o sensibilidad de la información que va a transmitir. A mayor frecuencia de renovación de claves mayor seguridad, aunque es necesario tener en cuenta posibles limitaciones impuestas por el tamaño de la red o el ancho de banda con el que se trabaja.
   El tiempo de vida de las Child SA no deberá ser mayor que el de las IKE SA y, en general, se recomiendan valores inferiores a 4 horas para las Child SA e inferiores a 24 h para las IKE SA.
10) Deberá activarse el PFS en IKEv2. Además se forzará la renovación de claves cada cierto tiempo o cada cierto volumen de datos.
11) AH (*Autentication Header*) es un protocolo opcional cuyo uso **no se recomienda**. En caso de que no sea necesaria protección de la confidencialidad se recomienda utilizar ESP con la opción de no cifrado.
12) Se recomienda el uso de ESP frente a AH. Se puede configurar sin cifrado o sin control de integridad, aunque no se recomienda.
13) Los algoritmos de cifrado simétrico más comúnmente utilizados en ESP son AES-GCM y AES-CBC o AES-CTR con HMAC-SHA. No obstante, siempre que sea posible se recomienda la utilización de AES-GCM (o de algún otro modo de cifra simétrica autenticado *"Encrypt-Then-MAC"*), dado que ofrece protección de confidencialidad y de integridad en un único proceso.
14) Si es necesario emplear NAT en las comunicaciones, deberá activarse la opción de NAT Transversal.
15) Todas las VPN que se establezcan en sistemas afectados por el ENS deberán configurarse de tal forma que solamente hagan uso de los algoritmos autorizados para el ENS. Estos algoritmos están descritos en la CCN-STIC-807. Además, también deberán utilizarse los mecanismos y protocolos descritos en la citada guía.
    Todos los productos con capacidad de establecer VPN que vayan a ser utilizados en sistemas clasificados deberán haber pasado una evaluación criptológica en la que se comprobará la fortaleza y correcta implementación los mecanismos y algoritmos utilizados, de acuerdo a lo establecido de la CCN-STIC-130.

8. COMPARACIÓN DE NIVELES DE SEGURIDAD Y LONGITUDES DE CLAVES

Nivel de seguridad o fortaleza (bits)	Longitud de clave RSA	Longitud de clave ECC	Longitud de clave simétrica
80	1024	160	80
112	2048	224	112
128	3072	256	128
192	7680	384	192
256	15360	512	256

Contacto

Correo electrónico CCN-PYTEC	**ccn-pytec@cni.es**
Twitter	**@CCNPYTEC**
LinkedIn	**https://www.linkedin.com/company/CCN-PYTEC**
Catálogo CPSTIC	**Enlace web**