TECHNICAL NOTES

Estudio de viabilidad sobre IPSec (en cooperación con DWD, Météo France, HNMS y KNMI):

Resumen y recomendaciones

Sección de Red y Seguridad
División de Informática
Mayo de 2003

European Centre for Medium-Range Weather Forecasts
Europäisches Zentrum für mittelfristige Wettervorhersage
Centre européen pour les prévisions météorologiques à moyen terme

Índice

Página

1 Introducción

Durante 2002, el ECMWF y cuatro Estados Miembros (Alemania, Grecia, Francia y Países Bajos) emprendieron pruebas sobre IPSec para evaluar la viabilidad de una red privada virtual (VPN) basada en IPSec como sistema de apoyo para la RCRDM y para la transferencia de volúmenes de datos que resulten excesivos para la capacidad de la RCRDM.

Dado que la mayoría de los sitios de la RCRDM tienen acceso a Internet, la utilización de un enlace VPN basado en IPSec como sistema de respaldo (backup) adicional ayudaría a garantizar la continuidad del servicio si fallara el enlace de la RCRDM y su correspondiente sistema de respaldo mediante RDSI.

La RCRDM es una red concebida específicamente para transferir datos en régimen operativo y en tiempo real, y las anchuras de banda asignadas para ello tienen un caudal de tráfico limitado. Cuando la capacidad de la RCRDM sea insuficiente, puede utilizarse Internet como recurso adicional para efectuar transferencias de datos. Sin embargo, conviene tener presente que:

- En Internet no existe el concepto de anchura de banda garantizada ni de calidad de servicio (QoS), y la red está expuesta a diversos tipos de ataques, incluidos los de denegación de servicio (DoS).
- Esporádicamente, puede haber en Internet interrupciones de servicio duraderas.

En el presente documento se informa de los resultados de las pruebas sobre IPSec, y se aportan directrices y recomendaciones para establecer conexiones seguras por Internet. Está dividido en cuatro partes:

La Parte 1 es una breve introducción a las redes privadas virtuales y a IPSec.
En la Parte 2 se describen las pruebas realizadas con IPSec.
En la Parte 3 se presentan los resultados de las pruebas.
En la Parte 4 se exponen en detalle las recomendaciones.

2 Consideraciones técnicas generales

2.1 Definición de VPN-IP (VPN mediante IP)

Una red privada virtual es un grupo de dos o más sistemas de computadora conectados "en condiciones seguras" a través de una red pública. Se puede instalar una VPN entre una máquina individual y una red privada (conexión a distancia de usuario a sitio) o entre redes privadas (de sitio a sitio). El tipo de seguridad difiere de un producto a otro, pero la mayoría de los expertos en seguridad coinciden en que las VPN deberían estar dotadas de encriptación, de una autentificación sólida de los usuarios o computadoras centrales distantes, y de mecanismos para ocultar o enmascarar información sobre la topología de la red privada frente a posibles atacantes desde la red pública.

2.2 El protocolo IPSec

IPSec es un protocolo de seguridad 'de extremo a extremo': toda la funcionalidad e inteligencia de la conexión VPN reside en los puntos extremos; es decir, o en una pasarela (gateway) o en la computadora central terminal.

La red IP del proveedor de servicio no es consciente de la existencia de la VPN-IP, ya que las tecnologías de 'tunelado' aseguran el transporte de datos de aplicación mediante encapsulación. Las direcciones fuente y destino de estos paquetes son las direcciones IP de los puntos extremos del túnel. Así, los paquetes son encaminados como cualquier paquete IP normal por la red IP compartida.

Hasta hace poco tiempo se estaban poniendo en servicio diversos protocolos de tunelado IP. En los últimos tres años, sin embargo, IPSec ha sido el protocolo de tunelado IP predominante, y es actualmente la tecnología preferida a la hora de establecer conectividad de sitio a sitio por una red pública. En un principio, IPSec fue desarrollado para establecer comunicaciones privadas por redes IP públicas. El protocolo IPSec permite establecer dos funciones de seguridad principales:

- Autentificación, que permite asegurar la autenticidad e integridad del paquete IP completo;
- Encriptación, que permite asegurar la confidencialidad de los datos transportados.

El protocolo IPSec permite definir un túnel entre dos pasarelas. Una pasarela IPSec consistiría normalmente en un encaminador (router) de acceso o un cortafuegos en el que esté implementado el protocolo IPSec. Las pasarelas IPSec están situadas entre la red privada del usuario y la red compartida del operador.

Los túneles IPSec se establecen dinámicamente y se liberan cuando no están en uso. Para establecer un túnel IPSec, dos pasarelas deben autentificarse y definir los algoritmos de seguridad y las claves que utilizarán para el túnel. El paquete IP original es encriptado en su totalidad e incorporado en encabezamientos de autentificación y encriptación IPSec. Se obtiene así la carga útil de un nuevo paquete IP cuyas direcciones IP de origen y destino son las direcciones IP de red pública de las pasarelas IPSec. Se establece así la separación lógica entre los flujos de tráfico de la VPN en una red IP compartida. Seguidamente, se utiliza un encaminamiento IP tradicional entre los extremos del túnel.

IPSec consigue estos objetivos mediante:

- Dos protocolos de seguridad de tráfico: el encabezamiento de autentificación (AH), que confiere integridad de los datos, y la carga útil de seguridad de encapsulación (ESP), que confiere integridad y confidencialidad de los datos.
- Un protocolo de gestión de clave criptográfica: el denominado 'intercambio de claves por Internet' (IKE), que se utiliza para negociar las conexiones IPSec.

Para una más amplia información sobre el protocolo IPSec, véase la lista de referencias del Anexo B

3 Las pruebas de IPSec

Los objetivos principales de dichas pruebas fueron:

- **Evaluar si es viable utilizar túneles IPSec para establecer conectividad de sitio a sitio:** Aunque se han escrito varios documentos sobre la implementación de IPSec y otras cuestiones al respecto, merecía la pena realizar la prueba para comprender a fondo el protocolo IPSec, hacerse una idea de su complejidad, y evaluar si era viable implementarlo en el contexto de la RCRDM.
- **Realizar pruebas de interoperabilidad de IPSec:** Los centros meteorológicos conectados a la RCRDM podrían disponer ya de ciertos equipos (router, cortafuegos, etc.) con capacidades IPSec. Aunque la interoperabilidad no sea actualmente un tema debatible, hay que verificar la interoperabilidad de diferentes dispositivos.
- **Definir recomendaciones de ámbito mundial:** Los sitios de la RCRDM que están estudiando la posible implementación de IPSec pueden utilizar este documento y sus recomendaciones como punto de partida.

3.1 Configuración de los parámetros de IPSec

Dado que no era viable probar todas las características y capacidades de IPSec, las pruebas se centraron en cierto número de ellas. Para cada parámetro IPSec se eligió una opción inicial:

Comparación entre el modo túnel y el modo transporte

Ambos protocolos, AH y ESP, operan en dos modos: modo transporte y modo túnel. Cada uno de estos modos tiene sus propias aplicaciones:

- El modo túnel se utiliza habitualmente para encriptar tráfico entre pasarelas IPSec seguras.
- El modo transporte se utiliza entre estaciones terminales que admiten IPSec, o entre una estación terminal y una pasarela, si ésta está considerada como computadora central.

Las pruebas tenían por objeto investigar las conexiones de sitio a sitio seguras, por lo que en el presente estudio sólo *se ha examinado el "modo túnel" en IPSec* (véase la Figura 1 *infra*).

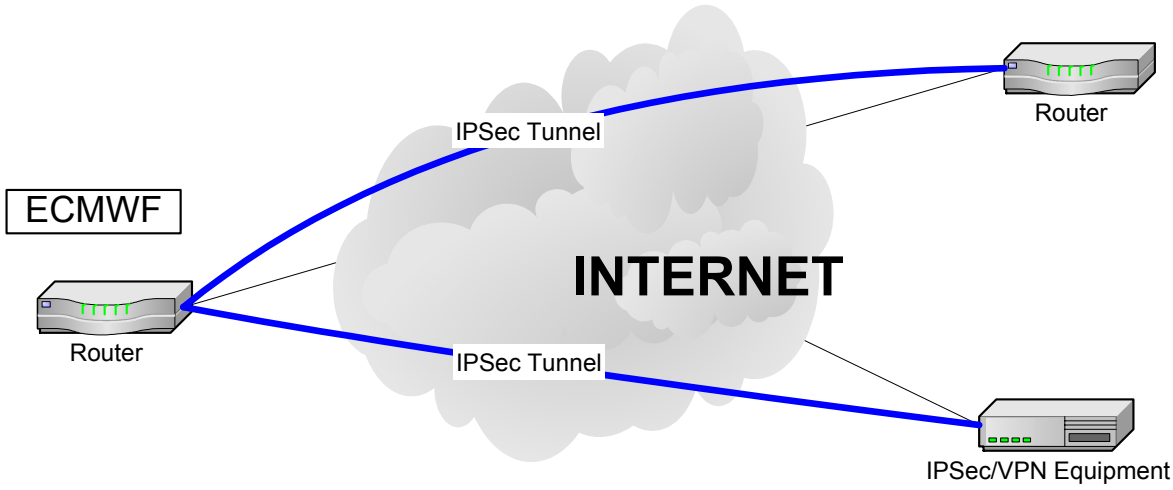

Figura 1 – Pruebas del "modo túnel" en IPSec

Intercambio de claves

Las claves en modo túnel con IPSec pueden ser gestionadas de manera manual o dinámica. Por razones de adaptabilidad a escala y de mantenimiento, durante las pruebas *se utilizó IKE para la gestión dinámica de las claves*.

Método de autentificación de dispositivos

El protocolo IKE es muy flexible y permite utilizar múltiples métodos de autentificación. Los dos comunicantes deben acordar un protocolo de autentificación común mediante un proceso de negociación. Los dos protocolos de autentificación principales son:

- **Clave pre-compartida (PreShared):**
  En cada uno de los comunicantes IPSec se configura una misma clave. Los comunicantes IKE se autentifican recíprocamente efectuando un troceo de datos y enviando éstos en clave mediante la clave PreShared configurada. Si el comunicante receptor es capaz de obtener el mismo troceo de manera independiente mediante su propia clave PreShared, tendrá la certeza de que ambos comunicantes comparten el mismo secreto, autentificando de ese modo al otro comunicante.
- **Firma RSA (Rivest, Shamir, Adleman):**
  Este sistema utiliza un método en virtud del cual cada dispositivo firma digitalmente un conjunto de datos y los envía a la otra parte. Las firmas RSA utilizan una CA (autoridad certificante) para generar un único certificado digital, que es asignado a cada comunicante a efectos de autentificación. El certificado digital realiza una función similar a la clave PreShared, pero ofrece mucha mayor seguridad.

Las claves PreShared son fáciles de implementar pero no son fácilmente redimensionables, ya que cada comunicante IPSec debe tener configurada la clave PreShared de cada uno de los demás comunicantes con los que establecerá una sesión. Además, las claves PreShared son menos seguras y están configuradas en formato de texto claro en ciertos equipos, por ejemplo en los routers Cisco.

Por consiguiente, *se utilizaron firmas RSA con certificados x509 v.3.*

Integridad y autenticidad de los datos

La integridad de los datos se obtiene incluyendo un condensado de mensaje (o huella dactilar) de los datos en los paquetes IPSec. Los condensados se calculan mediante funciones de troceo. Todos los dispositivos capaces de utilizar IPSec deberían admitir funciones de troceo HMAC-MD5 y HMAC-SHA, como se señala en la RFC (petición de comentarios) 2401. En consecuencia, se ignoraron otras funciones de troceo menos utilizadas. HMAC-MD5 y HMAC-SHA están basadas en MD5 y SHA, y en las posibilidades de encriptación adicionales del algoritmo HMAC. Con ello se pretende evitar interferir en el condensado de mensaje. MD5 produce un condensado de mensaje de 128 bits, mientras que SHA produce uno de 160 bits, por lo que SHA es una función de troceo más segura que MD5. Sin embargo, las variantes HMAC-SHA y HMAC-MD5 son truncadas en los 96 bits de mayor peso. Desde el punto de vista de la seguridad, el truncamiento presenta ventajas (el atacante dispone de menos información sobre el troceo), pero también desventajas (el atacante tendrá menos bits que predecir). En nuestra opinión, ambas versiones truncadas de HMAC-SHA y de HMAC-MD5 son suficientemente seguras para nuestras necesidades.

Para nuestra prueba *se utilizaron tanto HMAC-SHA como HMAC-MD5; nuestras preferencias se inclinaron ligeramente por HMAC-SHA*.

Encriptación de datos

En IPSec, la confidencialidad de los datos se obtiene mediante la utilización de algoritmos de encriptación simétricos y claves de sesión. Los algoritmos más habitualmente utilizados son:

- ESP-NULL: No se aplica encriptación alguna.
- DES (norma de encriptación de datos): Proporciona encriptación mediante una clave de 56 bits.
- 3DES (norma de triple encriptación de datos): Proporciona encriptación mediante una clave de 168 bits.
- AES (norma de encriptación avanzada): Proporciona encriptación mediante claves de 128, 192 y 256 bits de longitud.

Según RFC 2401, todos los dispositivos IPSec deberían admitir al menos ESP-NULL y DES. Sin embargo, DES está considerado como un algoritmo de encriptación débil, ya que utiliza una clave de encriptación corta, por lo que algunos vendedores desaconsejan su utilización, mientras que otros se niegan a darle soporte (concretamente, FreeS/Wan).
Así pues, para los fines de esta prueba *se utilizaron, siempre que fue posible, los modos de encriptación NULL (ausencia de encriptación) y 3DES*. DES se utilizó únicamente cuando no se disponía de 3DES.

> Una VPN/IPSec internacional vía Internet deberá cumplir la legislación de cada país (encriptación, tamaño de la clave...). Por consiguiente, cada sitio debería tener conocimiento de la política nacional sobre el particular antes de utilizar encriptación.

Intercambio de claves de sesión

Diffie-Hellman (DH) es un protocolo de criptografía de clave pública. Permite a dos partes establecer un secreto compartido entre ellas. DH se utiliza en IKE para establecer un secreto compartido que se utiliza como clave de sesión. Los grupos DH más habituales son:

- Grupo 1: Utiliza una clave pública de 768 bits para establecer un secreto compartido.
- Grupo 2: Utiliza una clave pública de 1024 bits para establecer un secreto compartido.

Para los fines de las pruebas *se utilizó un protocolo DH del Grupo 2*, ya que es más seguro y no crea información prescindible para los dispositivos IPSec.

3.2 Las pruebas de laboratorio

A fin de validar los diversos valores de parámetro de IPSec seleccionados, y antes de realizar cualquier prueba externa (por Internet), se creó en el ECMWF un entorno de prueba con objeto de realizar algunos experimentos preliminares. La finalidad de tales pruebas era familiarizarse con la configuración IPSec y con el proceso de adscripción a certificado.

En la Figura 2 se muestra la configuración de los dispositivos para la prueba.

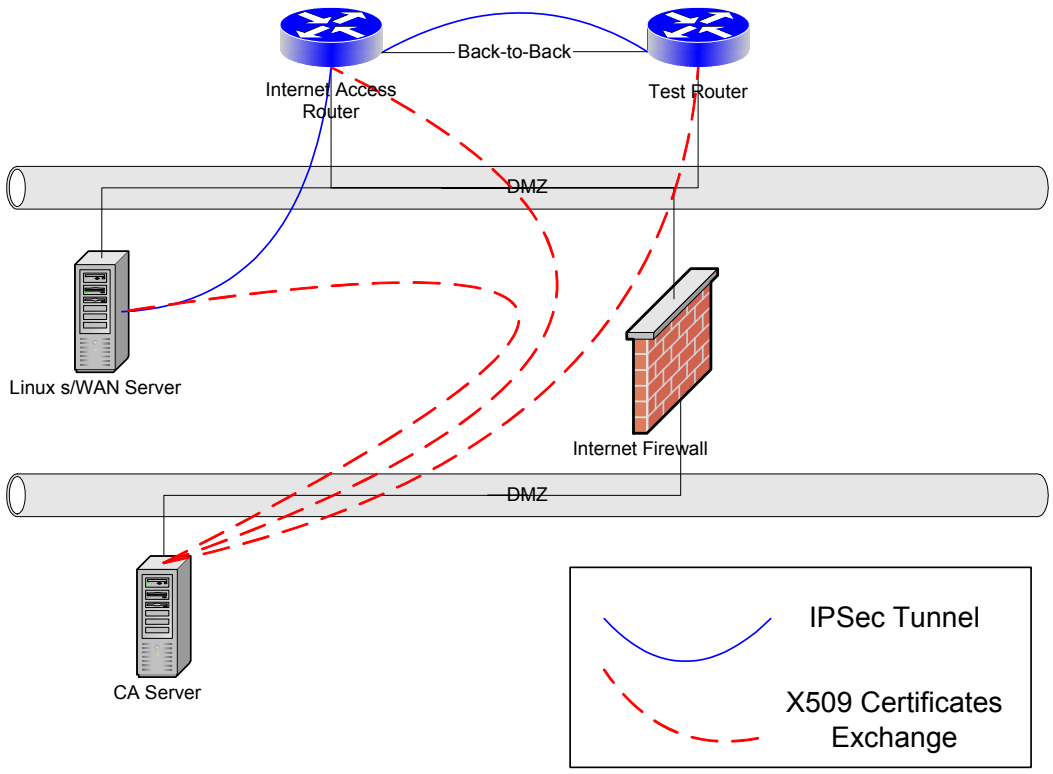

Figura 2 – Esquema de la prueba de la configuración de red

Con esta configuración conseguimos:

- Probar tres métodos de autentificación diferentes: claves PreShared, encriptación pública (RSA_ENCR), y claves públicas firmadas por una autoridad de certificación (RSA_SIG).
- Probar la incorporación y utilización de la certificación X509.
- Realizar una configuración IPSec básica: construir túneles con los parámetros IKE/IPSec elegidos.
- Probar una implementación de IPSec de dominio público: FreeS/WAN
- Probar la interoperabilidad de IPSec entre varios dispositivos.

La configuración de prueba se utilizó también durante las pruebas con Internet para reproducir ciertos problemas, con objeto de subsanarlos.

3.3 Pruebas en Internet

En la Figura 3 se indican esquemáticamente las pruebas de IPSec realizadas en la Internet pública. El objetivo de tales pruebas era establecer conexiones seguras entre el ECMWF y los Estados Miembros, y utilizarlas para transferir datos. En el anexo A se ofrecen varios ejemplos de configuraciones.

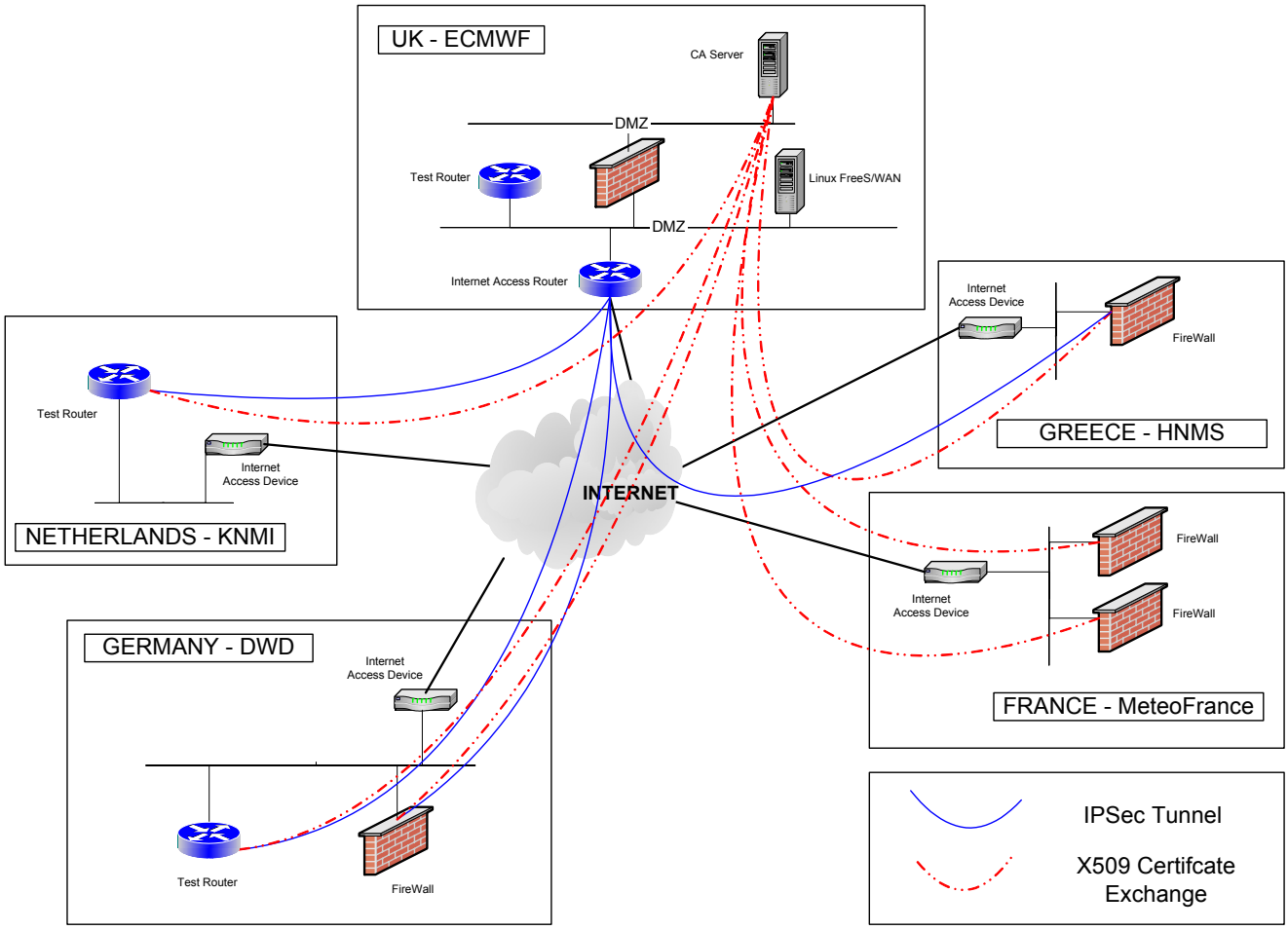

Figura 3 – Configuración de red para las pruebas en Internet

4 Resultados de la prueba

En las secciones siguientes se describen brevemente las cuatro pruebas realizadas con los Estados Miembros, y se indican algunas de las experiencias.

4.1 Prueba nº 1: adscripción a certificado y autentificación de dispositivos

La finalidad de esta prueba era averiguar en qué manera responderían los diferentes dispositivos durante el proceso de adscripción a certificado, y utilizar el certificado X509 para autentificar dispositivos. Cuando hubo problemas con la utilización de certificados X509 en algún dispositivo, se configuraron manualmente en el dispositivo las claves PreShared. La mayoría de los dispositivos probados consiguieron incorporar y utilizar certificados de autentificación[1].
Los principales problemas encontrados durante la prueba se debieron a que los dispositivos utilizaban diferentes métodos de adscripción a certificado (principalmente, descarga del URL y descarga "fuera de banda"), o formatos de certificado diferentes.

4.2 Prueba nº 2: Integridad de los datos

La finalidad de esta prueba era establecer conexiones IPSec básicas mediante un algoritmo HMAC (SHA y MD5) para comprobar la integridad de los datos. Para la negociación IKE se utilizó el certificado X509 descargado del servidor de la autoridad de certificación (AC). Excepto en el caso de FreeS/WAN, que no implementa el protocolo AH, todos los dispositivos probados pudieron establecer túneles IPSec HMAC para AH y ESP.

4.3 Prueba nº 3: Encriptación de datos

Esta prueba es una continuación de la nº 2; consiste en incorporar encriptación 3DES. Cuando no se dispuso de 3DES, se utilizó DES. Las pruebas dieron resultados satisfactorios. Sin embargo, es importante tener en cuenta que la capacidad de encriptación 3DES/DES depende de las versiones de hardware y software del dispositivo.

4.4 Prueba nº 4: Pruebas de efectividad

Con objeto de evaluar las repercusiones del tunelado IPSec en la CPU, se realizaron varias pruebas de FTP. Estas pruebas se realizaron con y sin tunelado IPSec.
La configuración indicada más abajo (Figura 5) fue la utilizada para realizar las pruebas de FTP; el router B representa un router distante genérico que garantiza la conexión de Internet hacia y desde un Estado Miembro.

[1] Equipo del punto de control FW1: se probó únicamente la incorporación del certificado. FW1 requiere una lista de revocación de control (CRL) para iniciar el proceso IPSec. En las pruebas no se incluyó la utilización de CRL. Ese tipo de pruebas se harán más adelante.

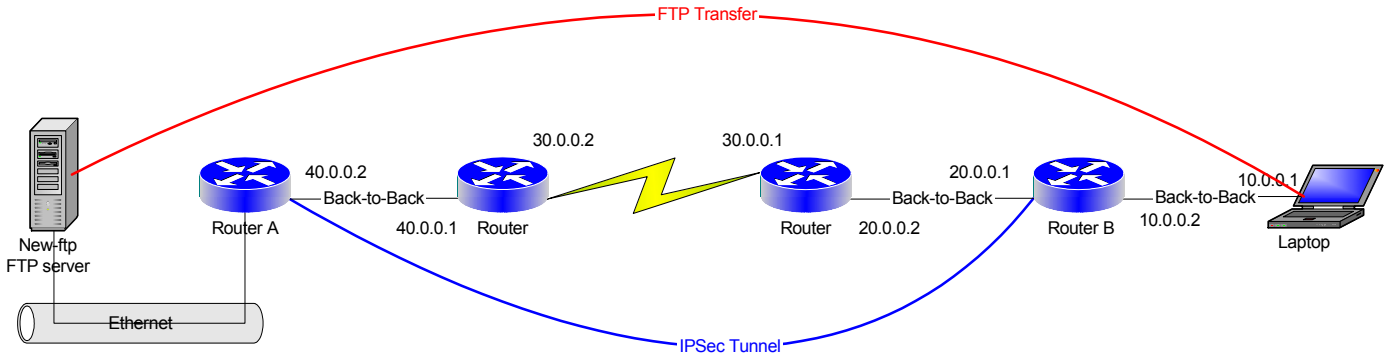

Figura 4 – Configuración en laboratorio para las pruebas de FTP

Se realizaron también pruebas en Internet entre el ECMWF y un cortafuegos PIX de Cisco en el Servicio Meteorológico de Alemania.

Las principales conclusiones de las pruebas de efectividad fueron:

- El protocolo IPSec influye considerablemente en el volumen de actividad de la CPU del dispositivo.
- Los túneles encriptados consumen más recursos de la CPU que los no encriptados.
- El algoritmo HMAC-MD5 consume ligeramente menos recursos de la CPU que el algoritmo HMAC-SHA.
- El protocolo ESP para integridad de datos consume el mismo volumen de recursos de la CPU que el protocolo AH.
- Un pequeño router con capacidades IPSec (como el Cisco 1605) no es adecuado para el tunelado IPSec cuando la velocidad de conexión a Internet es superior a 128 kb/s.

5 Recomendaciones

Las recomendaciones siguientes están basadas en los resultados de las pruebas descritas en la sección 3. Estas recomendaciones deberían ayudar a los sitios a establecer conexiones IPSec seguras en la Internet pública.

5.1 Autentificación de dispositivos

Se recomienda utilizar certificados X509 para la autentificación de dispositivos, en razón de las consideraciones siguientes:

- Es el método más seguro.
- Es el método más dimensionable.

Se recomienda además la generación de claves RSA de 1024 bits y la utilización del algoritmo DH del Grupo 2 (algoritmo de encriptación).

5.2 Integridad de los datos

Para la autentificación de paquetes pueden utilizarse tanto el protocolo AH como el ESP. Sin embargo:

- Las pruebas indicaron que ESP consume el mismo volumen de recursos de la CPU que AH.
- Sólo el protocolo ESP pueden asegurar la encriptación de paquetes (véase la sección 4.3).

Así pues, por razones de simplicidad se recomienda la utilización de HMAC con ESP para la autentificación de paquetes. Además, pueden utilizarse tanto ESP-HMAC-MD5 como ESP-HMAC-SHA.

5.3 Encriptación de datos

Dada la naturaleza de los datos (en este caso, meteorológicos), la encriptación no es estrictamente necesaria. Dado que la encriptación de datos consume recursos de la CPU, el establecimiento de autentificación de paquetes proporciona suficiente seguridad. Por ello, se recomienda la utilización de NULL con ESP. Esto significa que ESP se aplicará al paquete sin encriptación.
Si se necesitase encriptar los datos, se recomienda implementar ESP-3DES, que es más seguro que DES.

5.4 El equipo con capacidades IPSec

En vista de las recomendaciones precedentes (secciones 4-1 a 4-3), cuando se seleccione un dispositivo con capacidades IPSec para establecer una VPN habrá que tener en cuenta las consideraciones siguientes:

- Por razones de dimensionabilidad, el dispositivo debería tener capacidades IKE, y debería ser compatible con la norma de certificación X509.
- Es importante que el dispositivo admita el método de encriptación ESP_NULL.

- Si se considera la posibilidad de encriptar los datos, el equipo deberá tener capacidades 3DES. Además, habría que tener en cuenta que AES podría convertirse pronto en el estándar de encriptación de facto. Por ello, es deseable un equipo que tenga también capacidades AES, para poder prever las necesidades futuras.
- Para los sitios con conexión de alta velocidad a Internet, se recomienda un dispositivo VPN/IPSec con tarjeta de encriptación (tarjeta aceleradora), ya que reduce considerablemente el volumen de proceso de la CPU cuando se utiliza el protocolo IPSec.

Por último, las pruebas indicaron que es más fácil configurar equipos con capacidades IPSec que realizar una solución de dominio público. Sin embargo, podría contemplarse una implementación de código abierto, FreeS/WAN, teniendo presente que FreeS/WAN utiliza por defecto encriptación 3DES (se encontrará más información en http://www.freeswan.org).

5.5 Diseño de red

Al diseñar una implementación IPSec es necesario tener en cuenta una serie de directrices. La pasarela VPN debería estar siempre en una DMZ, y nunca dentro de la red "privada". Esto significa que el dispositivo VPN debe situarse entre un cortafuegos y la red externa (Internet); todo el tráfico que discurra entre el dispositivo VPN y la red interna privada debería pasar por un cortafuegos; véase la Figura 6.
Dado que el dispositivo VPN está situado en una DMZ, es importante configurar el cortafuegos para que permita el tráfico IPSec de entrada y de salida. En la tabla siguiente se indican los protocolos IP y los números de puerto TCP/UDP que el cortafuegos deberá respetar para que IPSec pueda operar:

Protocolo/Puerto	**Comentario:**
Protocolo IP 50	Protocolo ESP
Protocolo IP 51	Protocolo AH
UDP 500	Negociación IKE
UDP/TCP 10000	Tunelado NAT

Para implementar IPSec no es obligatorio utilizar un dispositivo IPSec dedicado. Es posible combinar las capacidades IPSec y de cortafuegos o las capacidades IPSec y de acceso a Internet, o las tres capacidades en un solo dispositivo.

En el diagrama siguiente (Figura 5) se representa una topología que utiliza un dispositivo dedicado VPN/IPSec además del router de acceso a Internet y del cortafuegos.

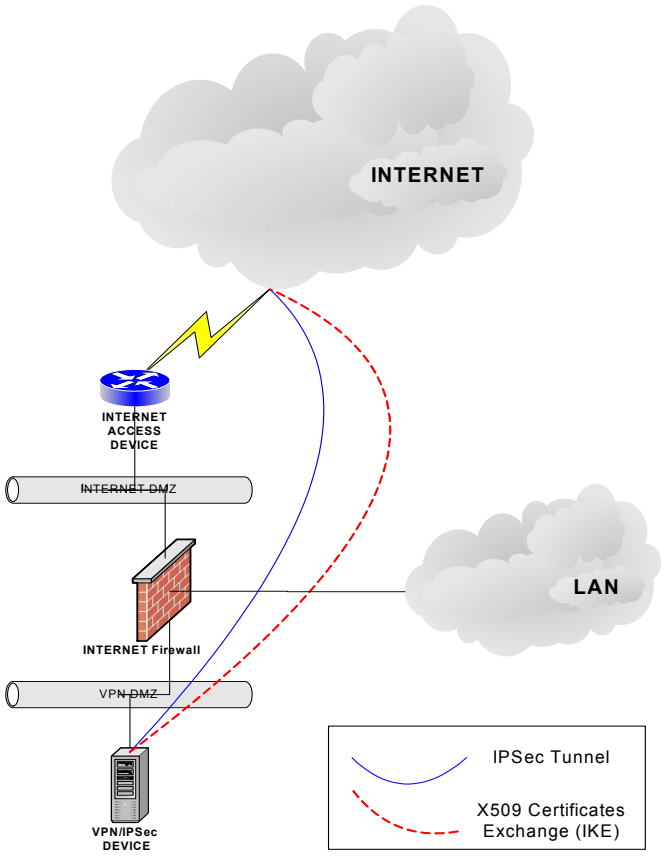

Figura 5 – Diseño de red VPN basado en un dispositivo VPN dedicado

6 Nota de agradecimiento

Al estudio y a la elaboración del presente documento han contribuido las personas siguientes:

Inge Essid, DWD

Ilona Glaser, DWD

Erwan Favennec, Météo France

Georgios Konstandinidis, HNMS

Frits van de Peppel, KNMI

Freerk Feunekes, KNMI

Carmine Rizzo, ECMWF

Ahmed Benallegue, ECMWF

Matteo dell'Acqua, ECMWF

Ricardo Correa, ECMWF

Tony Bakker, ECMWF

Pam Prior, ECMWF

Anexo A - Directrices y ejemplos en materia de configuraciones

A.1 Archivos de salida y de configuración para un router Cisco y PIX

El IOS de Cisco: Directrices para la adscripción a un certificado

Las principales tareas a considerar cuando se solicite un certificado de un router Cisco son las siguientes:

1- Configurar el nombre de la computadora central y el nombre de dominio del router: utilizar las instrucciones de configuración globales “hostname” e “ip domain-name”.
2- Establecer la fecha y hora del router: Asegurarse de que la zona horaria del router, así como la hora y la fecha, han sido adecuadamente configuradas mediante la instrucción "set clock”. El reloj deberá ser puesto en hora antes de generar pares de claves RSA y adscribirse al certificado, ya que tanto las claves como los certificados dependen de la hora.
3- Los pares de claves RSA deberán generarse módulo 1024: mediante la instrucción "crypto key generate rsa”, se generarán pares de claves RSA módulo 1024.
4- Declarar la AC y configurar sus parámetros:
   - Para declarar la AC: “crypto ca identity <identidad de la AC>”
   - Para configurar sus parámetros: "enrolment url <URL del servidor AC>” y “crl optional”
   - Para autentificar la AC: "ca authenticate <identidad de la AC>”
5- Solicitar un certificado X509: Al solicitar un certificado X509, responda "no" cuando le soliciten si desea incluir:
   - El número de serie del router
   - Una dirección IP en el apartado ‘Subject name’

El IOS de Cisco: Datos salientes de la operación de adscripción

Se indica a continuación el código resultante de la adscripción a un certificado en un router Cisco :

```
! En la primera etapa se genera la clave RSA
Cisco-Test(config)#crypto key generate rsa
The name for the keys will be: mys-Cisco .domain.top
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
A few minutes.

How many bits in the modulus [512]: 1024
Generating RSA keys ...
[OK]

! En la segunda etapa se genera el servidor AC
Cisco -Test(config)#ca iden
Cisco -Test(config)#crypto ca identity my-test
Cisco -Test(ca-identity)# enrollment url http://myca.domain.top/cgi-bin/openscep
Cisco -Test(ca-identity)# crl optional
Cisco -Test(ca-identity)#exit
Cisco -Test(config)#crypto ca authenticate my-test
Certificate has the following attributes:
Fingerprint: 8395FE5B C08238A7 FA6BFD76 727E84A7
% Do you accept this certificate? [yes/no]: yes

! En la tercera etapa se solicita un certificado del servidor AC
Cisco -Test(config)#crypto ca enrol my-test
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
Password to the CA Administrator in order to revoke your certificate.
  For security reasons your password will not be saved in the configuration.
  Please make a note of it.

Password:
Re-enter password:
```

```
% The subject name in the certificate will be: my-Cisco .domain.top
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [yes/no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto ca certificate' command will also show the fingerprint.

Cisco -Test(config)#exit
Cisco -Test#
! Una vez finalizadas estas tres etapas, se dispondrá de dos certificados en el router: el certificado AC y el certificado del router
Cisco -Test#show crypto ca certificates
CA Certificate
  Status: Available
  Certificate Serial Number: 01
  Key Usage: General Purpose
    EA =<16> ca-email@domain.top
     CN = Org
     O = Org
     L = Place
     ST = county
     C = Country
  Validity Date:
    start date: 08:51:38 GMT Apr 9 2002
    end   date: 08:51:38 GMT Apr 8 2012

Certificate
  Status: Available
  Certificate Serial Number: 3F
  Key Usage: General Purpose
  Subject Name
    Name: my-test.domain.top
  Validity Date:
    start date: 15:56:14 GMT Jun 12 2002
    end   date: 15:56:14 GMT Jun 13 2007
```

IOS de Cisco: Ejemplo de configuración IPSec

Se describe a continuación un ejemplo de configuración de túnel IPSec ESP-HMAC-SHA ESP-NULL:

```
hostname Cisco
!
!La zona horaria deberá ser correcta, ya que los certificados dependen de la fecha
clock timezone GMT 0
!
! En las líneas siguientes se describen el nombre y la dirección IP del servidor AC
ip host myca.domain.top 191.168.1.1
ip domain-name domain.top
!
! La instrucción 'ca identity' especifica el nombre local del servidor AC
crypto ca identity my-test
 enrollment url http://myca.domain.top/cgi-bin/openscep
 crl optional
!
! Las líneas siguientes son los certificados disponibles en el router
crypto ca certificate chain my-test
 certificate 36
  30820338 308202A1 A0030201 02020136 300D0609 2A864886 F70D0101 04050030
  ****
  B49B0FEF 07921B58 B9BD54B2 0713AE83 B6BA3CB4 B8D30EA8 95005EEA
  quit
 certificate ca 01
  30820379 308202E2 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  ****
  9A81DB7F 902EE833 800B9487 9634907E 9333BE95 88900068 7889AB95 51
  quit
!
! Los parámetros de política isakmp (ike) se utilizan cuando el router trata de establecer el túnel IKE
crypto isakmp policy 100
 group 2
!
crypto isakmp policy 200
 encr 3des
 group 2
!
! La instrucción "transform-set" define el tipo de túnel  IPSec que es posible establecer
```

```
crypto IPSec transform-set MoreSecure esp-sha-hmac esp-null
!
! Un cripto-mapa enlaza un conjunto de parámetros IPSec con la pasarela IPSec distante
crypto map IOS_IOS 10 IPSec-isakmp
 description To Cisco -Test internal router
 set peer 10.0.0.1
 set transform-set MoreSecure
 match address 151
!
! Por último, se aplica a la interfaz física un cripto-mapa que se utilizará para establecer túneles IPSec
interface FastEthernet4/0
 ip address 10.0.0.2 255.0.0.0
 crypto map IOS_IOS
!
! La lista de control de acceso del sitio espejo iniciará el establecimiento del túnel IPSec
access-list 151 permit ip host 192.168.1.2 host 192.168.2.1 log
end
```

PIX de Cisco: Ejemplo de configuración

Se describe a continuación un ejemplo de configuración de túnel IPSec ESP-HMAC-SHA ESP-NULL para un PIX de Cisco :

```
PIX Version 6.2(1)
hostname pix
domain-name domain.top
!
****
!
! La lista de control de acceso se utilizará para iniciar el establecimiento del túnel IPSec
access-list 101 permit ip host 192.168.3.1 host 192.168.1.2

! El protocolo IPSec deberá estar activado en el dispositivo
sysopt connection permit-IPSec
no sysopt route dnat

! La instrucción "transform-set" define el tipo de túnel IPSec que será posible establecer
crypto IPSec transform-set MoreSecure2 esp-null esp-sha-hmac

! Un cripto-mapa  define los parámetros IPSecs que serán negociados durante el establecimiento del túnel IPSec
crypto map ECMWF_MSS 50 IPSec-isakmp
crypto map ECMWF_MSS 50 match address 101
crypto map ECMWF_MSS 50 set peer 192.168.4.1
crypto map ECMWF_MSS 50 set transform-set MoreSecure
crypto map ECMWF_MSS interface outside

! Los parámetros de política isakmp (ike)se utilizan cuando el dispositivo trata de establecer el túnel IKE
isakmp enable outside
isakmp policy 10 authentication rsa-sig
isakmp policy 10 encryption des
isakmp policy 10 hash sha
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400

ca identity myca.domain.top 192.168.1.19:/cgi-bin/openscep
ca configure myca.domain.top ca 1 1 crloptional
```

A.2 Ejemplo de configuración FreeS/WAN

Ejemplo de archivo de configuración FreeS/WAN (IPSec.conf) para una configuración ESP-HMAC-SHA ESP-3DES:

```
# /etc/IPSec.conf – Archivo de configuración FreeS/WAN IPSec

# Pueden encontrarse ejemplos de configuración más elaborados y más variados
# en FreeS/WAN's doc/examples file, y en la documentación HTML.

# Configuración básica
config setup
        # ESTE VALOR DEBERÁ SER CORRECTO, o casi nada funcionará;
        # %defaultroute es adecuada para la mayoría de los casos simples.
        interfaces=%defaultroute
        # Controles de registro de depuración:  con "none" no habrá (casi) ninguno, con "all" habrá muchos.
        klipsdebug=none
        plutodebug=all
        # Utilizar auto= parámetros en las descripciones de la conexión para controlar las acciones de arranque.
```

```
        plutoload=%search
        plutostart=%search
        # Cerrar la conexión antigua cuando aparezca una nueva que utiliza el mismo identificador.
        uniqueids=yes

# valores por defecto para las descripciones posteriores de la conexión
conn %default
        # Grado de persistencia en el (re)envío de claves (0 equivale a 'alto').
        keyingtries=2
        # Autenticación de RSA con claves del DNS.
        # authby=secreto
        authby=rsasig
        #
        # utilizar certificados x509
        #
        leftrsasigkey=%cert
        rightrsasigkey=%cert
        #
        #pasarela de seguridad freeswan
        left=192.168.1.20
        leftsubnet=192.168.1.20/32
        leftid=@host.domain.top
        #
        keyexchange=ike


# a continuación, la configuración IPSec en la dirección hacia el router "Cisco "

conn rw1
  right=192.168.5.2
  rightid=@host.otherdomain.top
  rightsubnet=10.0.0.0/8
  ikelifetime=3600
  keylife=3600
  pfs=no
  auto=start
  esp=3des-sha-96
```

Anexo B - Referencias

- A cryptographic Evaluation of IPSec - Niels Ferguson and Bruce Schneier - Counterpass Internet Security, Inc.
- Applied Cryptography - Bruce Schneier - Wiley
- Cisco Secure VPN - Andre G. Mason - Cisco Press
- FreeS/WAN: http://www.freeswan.org
- Protocolo IPSec: http://www.ietf.org/html.charters/IPSec-charter.html
- RFCs IPSec- http://www.ietf.org/rfc.html
- IPSec Securing VPNs - Carlton R. Davis - RSA Press
- Consorcio de VPN: http://www.vpnc.org

Anexo C - Lista de abreviaturas

3DES	Norma de triple encriptación de datos
AES	Norma de encriptación avanzada
AH	Encabezamiento de autentificación
AC	Autoridad de certificación
CRL	Lista de revocación de certificados
DER	Reglas de codificación distinguida
DES	Norma de encriptación de datos
DH	Acuerdo sobre clave Diffie-Hellman
DWD	Deutscher Wetterdienst
ECMWF	Centro europeo de predicción meteorológica a medio plazo
ESP	Carga útil de seguridad de encapsulación
HMAC	Código de autentificación de mensaje troceado
HNMS	Servicio Meteorológico Nacional Helénico
IKE	Intercambio de claves por Internet
IPSec	Protocolo de seguridad IP
KNMI	Koninklijk Nederlands Meteorologisch Instituut
MD5	Condensado de mensaje 5
NAT	Traducción de direcciones de red
PEM	Correo de privacidad mejorada
PKI	Infraestructura de clave pública
QoS	Calidad de servicio
RFC	Petición de comentarios
RMDCN	Red de comunicación de datos meteorológicos regionales
RSA	Rivest, Shamir, Adleman
SHA	Algoritmo de troceo seguro