TECHNICAL NOTES

**NOTE TECHNIQUE**

# Étude de faisabilité IPSec (en coopération avec le DWD, Météo France, le HNMS et le KNMI) :

## Résumé et recommandations

Section réseaux et sécurité
Division informatique
Mai 2003

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

Centre européen pour les prévisions météorologiques à moyen terme
Shinfield Park, Reading, Berkeshire, RG2 9AX, Angleterre

# Table des matières

# 1 Introduction

En 2002, le CEPMMT et quatre de ses États Membres – l'Allemagne, la France, la Grèce et les Pays-Bas – ont exécuté des tests IPSec pour évaluer la possibilité d'utiliser un réseau privé virtuel avec le protocole IPSec (RPV IPSec) comme réseau de secours du Réseau régional de transmission de données météorologiques (RRTDM), mais aussi pour assurer le transfert des données quand la capacité du RRTDM est dépassée.

Comme la plupart des sites du RRTDM disposent d'un accès Internet, le fait d'utiliser une liaison RPV IPSec en tant que système de secours supplémentaire, en cas de panne de la liaison RRTDM et de sa liaison de secours RNIS, permettrait de mieux garantir la continuité du service.

Le RRTDM est un réseau spécialement conçu pour le transfert des données en temps réel à des fins d'exploitation, pour lequel ont été attribuées des bandes passantes permettant des débits limités. Il est possible d'avoir recours à l'Internet en complément du RRTDM pour exécuter des transferts de données lorsque la capacité du RRTDM se révèle insuffisante. Il convient néanmoins de prendre en compte les poins suivants :

- les notions de bande passante garantie et de qualité de service ne s'appliquent pas à l'Internet qui est exposé en outre à divers types d'attaques notamment les dénis de service ou attaques par saturation ;
- il arrive parfois que des pannes de longue durée se produisent sur l'Internet.

Les résultats des tests IPSec ainsi que des règles et des recommandations pour la sécurisation des connexions Internet sont fournis dans le présent document qui comporte quatre parties.

La première partie propose une brève introduction sur les réseaux privés virtuels et le protocole IPSec.
La deuxième partie décrit les tests IPSec que l'on a réalisés.
La troisième partie comprend les résultats de ces tests.
La quatrième partie fournit des recommandations détaillées.

# 2 Présentation technique de l'étude

## 2.1 Définition d'un RPV IP

Un réseau privé virtuel (RPV ou VPN – pour *Virtual Private Network*) est un service offrant une connexion sécurisée via un réseau public entre au moins deux systèmes informatiques. Un RPV peut être installé entre une machine et un réseau privé (utilisateur distant à site) ou entre deux réseaux privés (site à site). Les fonctions de sécurisation varient d'un produit à l'autre, mais la plupart des spécialistes des RPV conviennent qu'un RPV doit intégrer dans ses fonctionnalités le chiffrement, une bonne authentification des utilisateurs distants ou hôtes et des mécanismes permettant de cacher les informations sur la topologie du réseau privé à d'éventuels pirates ou agresseurs présents sur le réseau public.

## 2.2 Le protocole IPSec

IPSec est un protocole offrant une sécurité de bout en bout : toutes les fonctionnalités et tous les renseignements concernant la connexion RPV résident aux extrémités de la liaison, soit au niveau d'une passerelle soit à celui de l'hôte.

Le réseau IP d'un fournisseur d'accès n'est pas sensible à l'existence d'un RPV IP, car les techniques de tunnellisation permettent le transport de données d'applications par encapsulation. L'adresse source et l'adresse destination des paquets sont les adresses IP des extrémités du tunnel ainsi créé. Ces paquets sont donc acheminés comme tout autre paquet IP normal sur le réseau IP partagé.

Plusieurs protocoles de tunnellisation sous IP ont été créés par le passé, mais ces trois dernières années, IPSec s'est imposé au premier rang de ces protocoles, si bien qu'il est la technique la plus employée lorsqu'il s'agit de mettre en œuvre une liaison site à site sur un réseau public. Le protocole IPSec a été mis au point initialement pour sécuriser des communications privées sur des réseaux IP publics. Il comporte deux fonctions principales de sécurité :

- l'authentification – qui garantit l'authentification et l'intégrité de la totalité du paquet IP ;
- le chiffrement – qui garantit la confidentialité des données utiles ou charge utile.

Grâce au protocole IPSec, il est possible de définir un tunnel entre deux passerelles. Le plus souvent, la passerelle IPSec est un routeur d'accès distant ou un pare-feu sur lequel est mis en œuvre le protocole IPSec. Les passerelles IPSec se situent entre le réseau privé de l'utilisateur et le réseau partagé de l'entreprise de télécommunications.

Un tunnel IPSec est créé de façon dynamique ; il disparaît s'il n'est pas utilisé. Pour créer un tunnel IPSec, deux passerelles doivent s'authentifier et définir les algorithmes et les clés de sécurité dont elles vont se servir pour mettre en place le tunnel. La totalité du paquet IP initial est chiffré et « enveloppé » entre des en-têtes d'authentification et de chiffrement IPSec, si bien qu'il devient la charge utile d'un nouveau paquet IP dont les adresses IP de source et de destination sont les adresses IP des passerelles IPSec sur le réseau public. Ce processus permet la séparation logique du trafic du RPV sur un réseau IP partagé. Un routage IP normal s'opère entre les deux extrémités du tunnel.

Les fonctionnalités d'IPSec reposent sur les protocoles suivants :

- deux protocoles assurant la sécurité du trafic – le protocole d'authentification AH (*Authentication Header*) qui garantit l'intégrité des données et le protocole de confidentialité ESP (*Encapsulation Security Payload*) qui garantit l'intégrité et la confidentialité des données ;
- le protocole de gestion des clés de chiffrement IKE (*Internet Key Exchange*), utilisé pour négocier les connexions IPSec.

Pour obtenir davantage de détails sur le protocole IPSec, se reporter à la liste de références de l'annexe B.

# 3 Les tests IPSec

Voici quels étaient les principaux objectifs des tests réalisés :

- **Évaluer la possibilité d'utiliser des tunnels IPSec pour établir des liaisons site à site :**
  Certes plusieurs documents sont parus au sujet de la mise en œuvre du protocole IPSec et de ses diverses applications, mais il paraissait néanmoins utile de vérifier le fonctionnement de ce protocole afin de bien le cerner, d'en apprécier la complexité et d'évaluer s'il cadrait avec le contexte du RRTDM.
- **Vérifier l'interopérabilité du protocole IPSec :**
  Les centres météorologiques connectés au RRTDM disposent sans doute déjà de matériel du type routeur, pare-feu, etc. pouvant accepter le protocole IPSec. Il paraissait bon de vérifier l'interopérabilité du protocole, même si la question ne se pose pas aujourd'hui.
- **Formuler des recommandations valables dans le monde entier :**
  Dans les sites du RRTDM où l'on envisage de mettre en œuvre le protocole IPSec, on pourra ainsi se référer, comme point de départ, au présent document et aux recommandations qu'il contient.

## 3.1 Paramétrage du protocole IPSec

La vérification de toutes les caractéristiques du protocole IPSec se révélant impossible, les tests ont porté sur certains modes de fonctionnement, une option initiale étant retenue pour chaque paramètre.

### Mode tunnel ou mode transport

Les deux protocoles AH et ESP autorisent deux types de mise en œuvre : le mode « transport » et le mode « tunnel ». A chacun de ces modes correspondent certaines applications :

- le mode tunnel sert habituellement au chiffrement du trafic entre deux passerelles IPSec sécurisées ;
- le mode transport est utilisé entre hôtes finals IPSec ou un hôte final et une passerelle, si la passerelle est considérée comme un hôte.

Comme les tests avaient pour but l'évaluation de liaisons sécurisées site à site, seul le *mode tunnel IPSec* (voir la figure 1) a été retenu dans le cadre de l'étude.

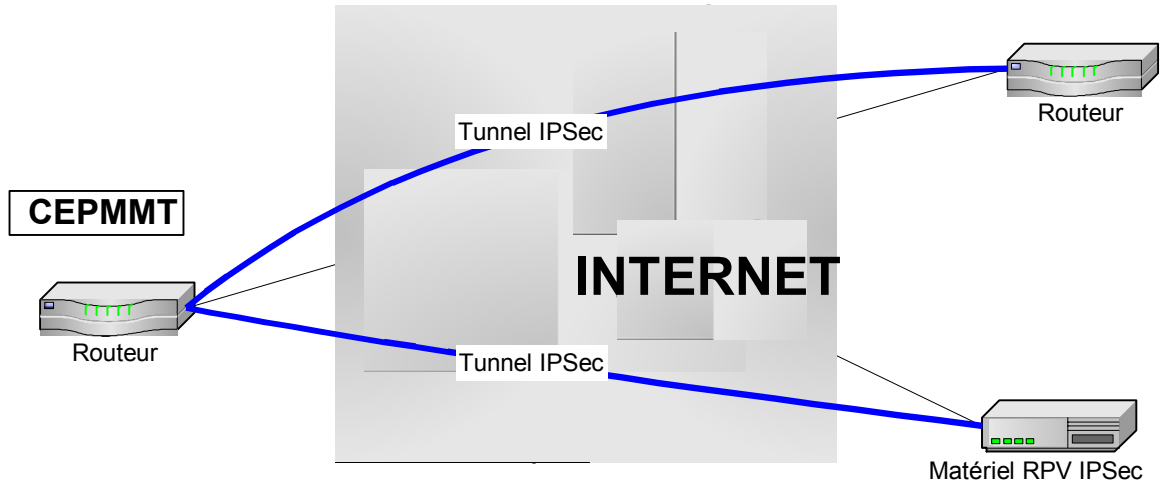


**Figure 1 – Tests du mode tunnel IPSec**

### Échange de clés

IPSec autorise une gestion soit manuelle soit dynamique des clés servant à la création d'un tunnel. Pour des raisons d'extensibilité et de maintenabilité, *on a choisi d'utiliser une gestion dynamique des clés par le protocole IKE* au cours des tests.

### Méthode d'authentification d'un matériel

Disposant d'une grande souplesse d'utilisation, le protocole IKE reconnaît de multiples méthodes d'authentification. Par un processus de négociation, deux entités homologues doivent s'entendre sur une méthode commune d'authentification pour établir une liaison. Les deux principaux modes d'authentification sont les suivants :

- **Partage préalable de clé :**
  La même clé est configurée sur chacune des entités homologues IPSec. Les entités homologues IKE s'authentifient l'une à l'autre en transmettant après calcul des données hachées à l'aide de la clé configurée préalablement partagée. Si l'entité qui reçoit ces données est capable de recréer le même message haché à l'aide de la clé préalablement partagée dont elle dispose, elle sait alors que le même « secret » est partagé et cela lui permet d'authentifier l'autre entité.
- **Signature RSA (Rivest, Shamir, Adleman) :**
  Cette méthode utilise une signature numérique. Chaque entité appose une signature numérique à un groupe de données qu'elle envoie à l'autre partie. Les signatures RSA font intervenir une autorité de certification (AC) dite aussi tierce partie de confiance, qui délivre un certificat numérique unique attribué à chaque entité pour authentification. Le certificat numérique remplit la même fonction que la clé secrète partagée, mais garantit une bien meilleure sécurité.

Les clés secrètes partagées sont faciles à mettre en œuvre mais pèchent par un manque de souplesse, ce dont il faut tenir compte puisque chaque entité IPSec doit être configurée à l'aide de la clé secrète partagée avec chacune des autres entités avec lesquelles une session est établie. Les clés secrètes partagées offrent en outre un niveau de sécurité relativement moins élevé et sont configurées en format texte, en clair, dans certains appareils, un routeur Cisco par exemple.

Par conséquent les tests ont porté sur le mode d'authentification suivant : *signatures RSA avec certificats x509 v.3* .

### Intégrité et authenticité des données

L'intégrité des données est garantie par l'inclusion dans les paquets IPSec d'un condensé du message, sorte d'empreinte digitale de son contenu. Le condensé de message est produit à l'aide d'un algorithme de hachage. Tous les appareils compatibles IPSec devraient être dotés des fonctions de hachage HMAC-MD5 et HMAC-SHA, comme cela est indiqué dans la RFC (*Request For Comments*) 2401. C'est pourquoi il a été décidé d'ignorer les autres fonctions de hachage moins courantes. Les fonctions HMAC-MD5 et HMAC-SHA combinent les algorithmes MD5 et SHA aux fonctions de chiffrement supplémentaires de l'algorithme HMAC. On s'assure ainsi de l'intégrité du condensé de message. L'algorithme MD5 produit un condensé de 128 bits, tandis que celui produit par SHA est de 160 bits, c'est pourquoi la fonction de hachage SHA offre davantage de sécurité que MD5. Il faut noter toutefois que les variantes HMAC-MD5 et HMAC-SHA utilisées sont tronquées pour ne conserver que les 96 bits les plus significatifs. A des fins de sécurité, cette troncature présente des avantages – moins d'informations dans la partie hachée à la disposition des agresseurs éventuels – mais aussi des inconvénients – moins de bits à prévoir pour les mêmes agresseurs. Compte tenu des besoins fixés, on estime que les deux versions tronquées HMAC-SHA et HMAC-MD5 offrent un niveau de sécurité suffisant.

Dans le cadre des tests réalisés, *on a utilisé tant HMAC-SHA que HMAC-MD5, avec une légère préférence pour HMAC-SHA*.

### Chiffrement des données

Le protocole IPSec assure la confidentialité des données à l'aide d'algorithmes de chiffrement symétrique et de clés de session. Les algorithmes les plus utilisés sont :

- ESP-NULL – pas de chiffrement ;
- DES (*Data Encryption Standard*) – chiffrement à l'aide d'une clé de 56 bits ;
- 3DES (*Triple Data Encryption Standard*) – chiffrement à l'aide d'une clé de 168 bits ;
- AES (*Advanced Encryption Standard*) : chiffrement à l'aide d'une clé de longueur variable : 128, 192 ou 256 bits.

En application de la RFC 2401, tous les matériels compatibles IPSec devraient permettre d'utiliser au moins les deux solutions ESP-NULL et DES. On estime cependant que l'algorithme DES n'offre qu'un chiffrement de faible niveau en raison de la faible longueur de la clé utilisée. Certains vendeurs déconseillent d'utiliser cet algorithme et des fabricants refusent de l'intégrer dans leurs produits (FreeS/Wan).

Pour les besoins de ces tests, *on a donc utilisé les deux solutions suivantes : aucun chiffrement (NULL) et le chiffrement 3DES quand cela était possible*. DES n'a été utilisé que lorsque l'on ne pouvait utiliser 3DES.

> La mise en place d'un RPV IPSec international via Internet exige le respect de la législation propre à chaque pays (chiffrement, longueur des clés, etc.). Il est donc conseillé au personnel de chaque site de bien connaître cette législation avant d'utiliser le chiffrement.

### Échange de clés de session

L'algorithme de Diffie-Hellman (DH) est un protocole de chiffrement à clé publique. Il permet à deux parties de posséder en commun une clé secrète. Ainsi l'algorithme DH est utilisé au sein du protocole IKE pour créer une clé secrète partagée utilisée comme clé de session. Les groupes DH les plus utilisés sont :

- le groupe 1 qui utilise une clé publique de 768 bits pour créer la clé secrète partagée,
- le groupe 2 qui utilise une clé publique de 1 024 bits pour créer la clé secrète partagée.

Pour les besoins des tests réalisés, *c'est le groupe DH 2 qui a été retenu* car il est plus sûr et n'engendre pas de surcharge sur les matériels IPSec.

## 3.2 Tests en laboratoire

Afin de valider le paramétrage choisi des fonctionnalités du protocole IPSec, et avant de passer à des tests externes (sur l'Internet), on avait décidé de procéder à des essais préliminaires dans un environnement conçu à cet effet pour se familiariser avec la configuration IPSec et avec le processus de délivrance de certificats de sécurité.

La figure 2 montre la configuration de l'environnement de test.

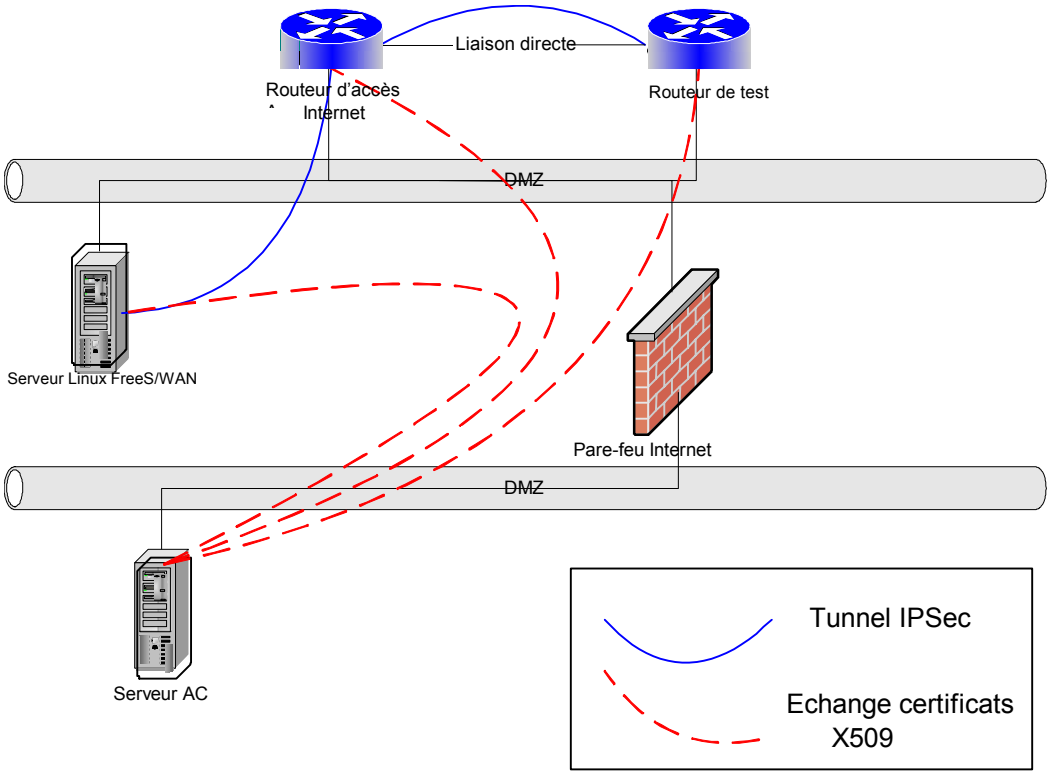


**Figure 2 – Configuration du réseau pour l'environnement de test**

Cette configuration a permis :

- de tester trois méthodes d'authentification différentes – clés secrètes partagées, chiffrement par clé publique (RSA_ENCR) et chiffrement par clé publique signée par une autorité de certification (RSA_SIG) ;
- de tester le processus de délivrance de certificats X509 et l'utilisation de ces certificats ;
- d'établir des configurations IPSec de base – créer des tunnels avec le paramétrage IKE-IPSec choisi ;
- de tester la mise en œuvre d'une version gratuite du protocole IPSec : FreeS/WAN
- de tester l'interopérabilité du protocole IPSec sur plusieurs matériels.

L'environnement de test a également été utilisé au cours des tests sur l'Internet afin de reproduire les problèmes rencontrés pour y apporter une solution.

## 3.3 Tests sur l'Internet

La figure 3 propose une vue d'ensemble des tests IPSec réalisés sur le réseau public Internet. Il s'agissait d'établir des liaisons sécurisées entre le CEPMMT et les États Membres pour le transfert de données. L'annexe A regroupe des exemples des configurations utilisées.

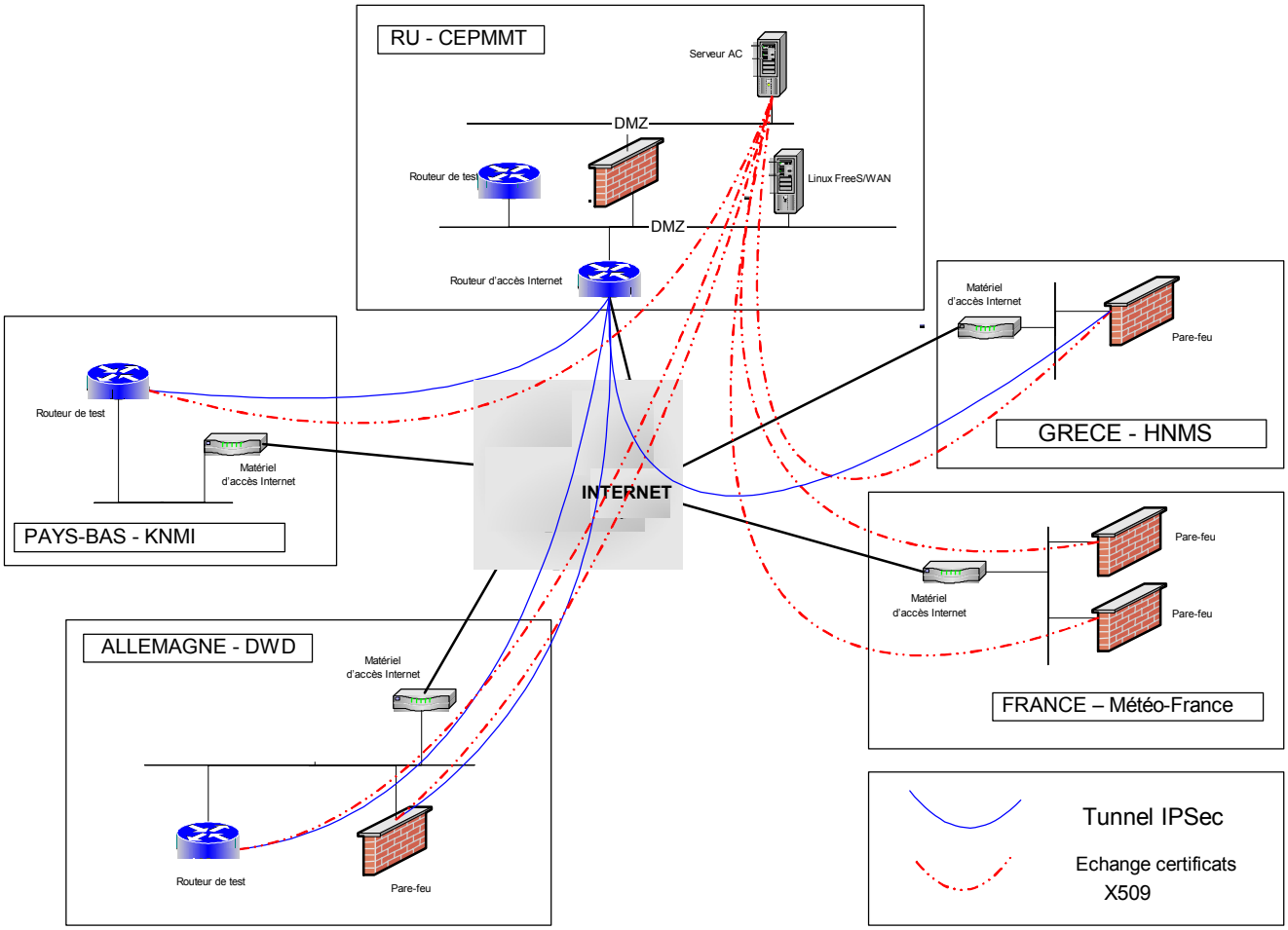


**Figure 3 – Configuration du réseau pour les tests sur l'Internet**

# 4 Résultats des tests

Les quatre tests réalisés avec les États Membres sont décrits brièvement dans ce qui suit ; certains résultats sont soulignés.

## 4.1 Test n° 1 : Délivrance de certificats et authentification des matériels

Il s'agissait d'analyser le comportement des différents matériels au cours du processus de délivrance de certificats et l'utilisation de certificats X509 pour l'authentification de ces matériels. Lors du test, les clés secrètes partagées ont été configurées manuellement quand l'utilisation de certificats X509 posait un problème. Pour la plupart des matériels testés, la délivrance et l'utilisation de certificats pour les besoins d'une authentification n'ont pas posé de problèmes[1].
Les principales difficultés rencontrées sont dues au fait que les différents matériels emploient des méthodes différentes pour la délivrance de certificats (surtout par téléchargement URL et « hors bande ») et différents formats de certificats.

## 4.2 Test n° 2 : Intégrité des données

Il s'agissait d'établir des connexions IPSec de base à l'aide de l'algorithme HMAC (SHA et MD5), pour vérifier l'intégrité des données. Pour la négociation IKE, les certificats X509 étaient téléchargés à partir du serveur AC. Tous les dispositifs testés ont pu établir des tunnels IPSec HMAC AH et ESP à l'exception du FreeS/WAN qui n'accepte pas le protocole AH.

## 4.3 Test n° 3 : Chiffrement des données

Il s'agissait de la suite logique du test n° 2, auquel on ajoutait ainsi le chiffrement 3DES. Quand 3DES n'était pas disponible, on a utilisé le chiffrement DES. Les résultats obtenus sont bons. Il importe cependant de noter que la possibilité d'utiliser le chiffrement 3DES ou DES varie en fonction du matériel et de la version du logiciel dont on dispose.

## 4.4 Test n° 4 : Performances

Un jeu de tests FTP a été réalisé pour évaluer la charge d'une tunnellisation IPSec sur l'unité centrale. Ce jeu de tests comprenait plusieurs tests FTP avec ou sans tunnel IPSec.
Les tests FTP ont porté sur la configuration illustrée à la figure 4 ; le routeur B représente un modèle distant type qui assure la connexion Internet (dans les deux sens) d'un État Membre.

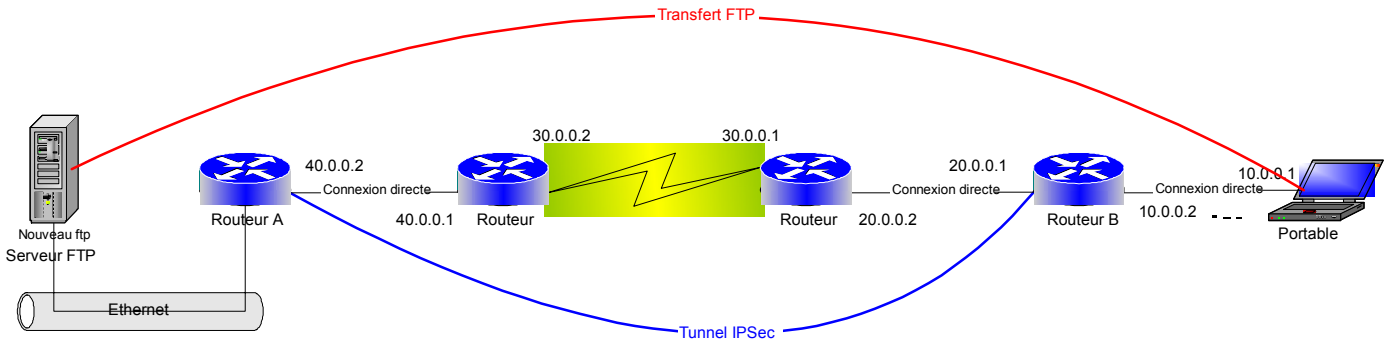


**Figure 4 – Configuration des tests FTP en laboratoire**

[1] Dans le cas du matériel CheckPoint FW1, le test n'a porté que sur la délivrance de certificats. Le FW1 nécessite une liste des certificats révoqués (LCR) pour lancer le processus IPSec, mais le programme des tests ne prévoyait pas l'utilisation de LCR. Cette solution sera étudiée à une date ultérieure.

Des tests ont été réalisés également sur l'Internet entre le CEPMMT et un pare-feu Cisco PIX au DWD en Allemagne.

Voici les principales conclusions à tirer de ces tests de performances :

- L'emploi du protocole IPSec représente une charge non négligeable pour l'unité centrale du matériel utilisé.
- Un tunnel avec chiffrement est plus lourd qu'un tunnel sans chiffrement.
- L'algorithme HMAC-MD5 est légèrement moins lourd que l'algorithme HMAC-SHA.
- Le protocole ESP qui assure l'intégrité des données est tout aussi lourd que le protocole AH.
- Un petit routeur acceptant IPSec (le Cisco 1605 par exemple) ne permet pas de créer de tunnel IPSec quand le débit de la connexion Internet est supérieur à 128 kb/s.

# 5 Recommandations

Les recommandations suivantes se fondent sur les résultats obtenus lors des tests décrits à la section 3. Elles doivent permettre aux sites concernés d'établir des connexions sécurisées IPSec sur le réseau public Internet.

## 5.1 Authentification des matériels

Pour l'authentification des matériels, il est recommandé d'utiliser les certificats X509 car :

- c'est la méthode la plus sûre,
- c'est la méthode la plus souple.

Il est en outre recommandé d'utiliser les clés RSA 1024 bits et l'algorithme de chiffrement DH groupe 2.

## 5.2 Intégrité des données

Il est possible d'utiliser aussi bien le protocole AH que le protocole ESP pour l'authentification des paquets. Toutefois :

- les tests ont montré que ESP n'est pas plus lourd que AH pour les unités centrales ;
- seul le protocole ESP autorise le chiffrement des paquets (voir la section 4.3).

Pour des raisons de simplicité, il est donc recommandé d'utiliser ESP HMAC pour l'authentification des paquets. La combinaison ESP-HMAC-MD5 fonctionne tout aussi bien que la combinaison ESP-HMAC-SHA.

## 5.3 Chiffrement des données

Compte tenu de la nature des données (météorologiques), il n'est pas absolument nécessaire d'avoir recours au chiffrement. Comme le chiffrement des données constitue une charge supplémentaire pour les unités centrales, le niveau de sécurité garanti par une authentification des paquets semble suffisant. Il est donc recommandé d'utiliser ESP-NULL, ce qui signifie que le protocole ESP s'applique au paquet sans chiffrement des données.
S'il devenait indispensable de chiffrer les données, il serait recommandé alors de mettre en œuvre la combinaison ESP-3DES qui est plus sûre que ESP-DES.

## 5.4 Matériel compatible IPSec

Les recommandations qui précèdent (sections 4.1 à 4.3) étant prises en compte, il convient aussi de bien examiner les points suivants lorsqu'il s'agit de sélectionner un matériel compatible IPSec pour mettre en œuvre un RPV :

- Pour des raisons d'extensibilité, il serait bon que le dispositif accepte le protocole IKE et puisse accueillir également le standard de certificat X509.
- Il importe que le matériel accepte la méthode de chiffrement ESP-NULL.
- Si l'on veut pouvoir chiffrer les données, il doit aussi accepter le protocole 3DES. Par ailleurs, il se peut fort bien que, dans la pratique, AES devienne bientôt le standard en matière de chiffrement. Il serait bon d'en tenir compte et de se procurer un matériel acceptant ce standard si l'on veut anticiper les besoins futurs.
- Dans les sites qui disposent d'une connexion Internet à haut débit, il est recommandé de se procurer un matériel spécialement conçu pour les RPV IPSec, doté d'une carte de chiffrement

(carte accélératrice), car cela permet de bien réduire la charge sur l'unité centrale due à l'utilisation du protocole IPSec.

Pour conclure, les tests ont montré qu'il était plus facile de configurer un matériel compatible IPSec que de mettre en œuvre une solution gratuite. On pourra néanmoins envisager de mettre en œuvre le code source libre FreeS/WAN, à condition de garder à l'esprit que celui-ci met en œuvre le chiffrement 3DES par défaut (se reporter à http://www.freeswan.org pour obtenir de plus amples détails).

## 5.5 Structure du réseau

Pour concevoir la mise en œuvre du protocole IPSec, il y a lieu d'appliquer un certain nombre de principes. La passerelle RPV doit toujours se trouver dans une zone DMZ et ne jamais faire partie du réseau privé interne. Cela signifie qu'il faut placer le matériel RPV quelque part entre un pare-feu et le réseau externe (Internet) et que l'ensemble du trafic entre le matériel RPV et le réseau privé interne doit traverser un pare-feu (voir la figure 5). Compte tenu de cette contrainte, il importe de configurer le pare-feu pour qu'il laisse passer le trafic IPSec dans les deux sens. Dans le tableau qui suit, sont indiqués les protocoles IP et les numéros de port TCP/UDP que le pare-feu doit accepter pour que le protocole IPSec fonctionne.

| **Protocole, Port** | **Remarque** |
|---|---|
| protocole IP 50 | protocole ESP |
| protocole 51 | protocole AH |
| UDP 500 | négociation IKE |
| UDP/TCP 10000 | tunnellisation NAT |

Il n'est pas obligatoire d'utiliser un matériel conçu uniquement pour IPSec pour mettre en œuvre ce protocole. Un même matériel pourra combiner plusieurs fonctions : IPSec et pare-feu, IPSec et accès Internet ou encore ces trois fonctions.

Le diagramme de la figure 5 représente la topologie correspondant à l'installation d'un matériel spécialisé RPV IPSec en association avec un routeur d'accès Internet et un pare-feu.

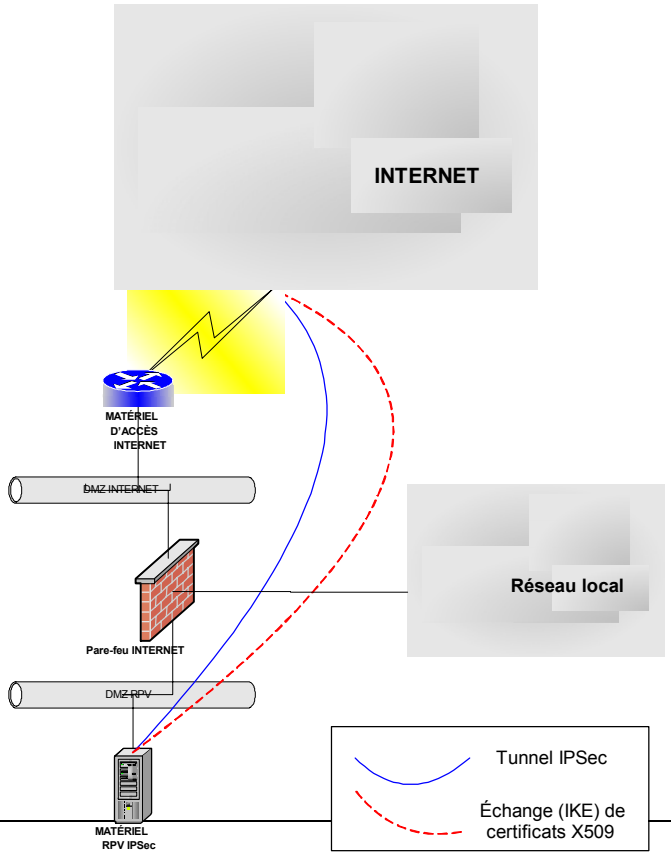

**Figure 5 – Structure d'un RPV utilisant un matériel spécial RPV**

# 6 Remerciements

Voici la liste des personnes qui ont contribué à l'étude et à la création du présent document :

Inge Essid, DWD
Ilona Glaser, DWD
Erwan Favennec, Météo France
Georgios Konstandinidis, HNMS
Frits van de Peppel, KNMI
Freerk Feunekes, KNMI
Carmine Rizzo, CEPMMT
Ahmed Benallegue, CEPMMT
Matteo dell'Acqua, CEPMMT
Ricardo Correa, CEPMMT
Tony Bakker, CEPMMT
Pam Prior, CEPMMT

# Annexe A - Configuration – règles et exemples

## A.1 Données de sortie et fichiers de configuration d'un routeur Cisco et d'un pare-feu Cisco PIX

### Cisco IOS : règles s'appliquant à la délivrance de certificats

Voici les points principaux à prendre en compte pour demander un certificat à partir d'un routeur Cisco :

1- Configurer le nom d'hôte et le nom de domaine du routeur – Se servir des commandes générales de configuration « hostname » et « ip domain-name ».
2- Régler la date et l'heure sur le routeur – Vérifier que le fuseau horaire, l'heure et la date du routeur ont été configurés avec exactitude à l'aide de la commande « set clock ». Les processus de création de bi-clés RSA et de délivrance de certificats nécessitent une horloge bien réglée en raison de la durée de validité limitée des clés et des certificats.
3- Les bi-clés RSA doivent être établis avec un modulo de 1 024 bits – Se servir de la commande « crypto key generate rsa » pour créer les bi-clés RSA avec un modulo de 1 024 bits.
4- Déclarer l'AC et configurer ses paramètres :
   - pour déclarer l'AC – « crypto ca identity <CA identity> »,
   - pour configurer ses paramètres – « enrolment url <CA server URL> » et « crl optional »,
   - pour authentifier l'AC – « ca authenticate <CA identity> ».
5- Demander un certificat X509 – au cours du processus, répondre « no » aux questions suivantes du routeur :
   - *Include the router serial number in the subject name? [yes/no]*
   - *Include an IP address in the subject name? [yes/no]*

### Cisco IOS : données de sortie pour la délivrance de certificats

Voici les données de sortie d'un routeur Cisco pour le processus de délivrance de certificats.

```
! The first step is to generate the RSA key
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]

! The second step is to identify the CA server
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

! The third step is to request a certificate from the CA server
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#
! Once the 3 steps are completed, two certificates are available in the router: the CA certificate and the router's certificate
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
```

## Cisco IOS : exemple de configuration IPSec

Voici un exemple de tunnel IPSec ESP-HMAC-SHA ESP-NULL.

```
hostname Cisco
!
! The time zone must be accurate, as the certificates are time sensitive
clock timezone GMT 0
!
! The following lines describe the CA server name and IP address
ip host myca.domain.top 191.168.1.1
ip domain-name domain.top
!
! CA identity command specifies the local name of the CA server
crypto ca identity my-test
 enrollment url http://myca.domain.top/cgi-bin/openscep
 crl optional
!
! The following lines are the certificates available in the 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
!
! The isakmp (ike) policy parameters are used when the router tries to establish the IKE tunnel
crypto isakmp policy 100
 group 2
!
crypto isakmp policy 200
 encr 3des
 group 2
!
! "transform-set" command defines which kind of IPSec tunnelit  is possible to establish
crypto ipsec transform-set MoreSecure esp-sha-hmac esp-null
!
! A crypto-map links a set of IPSec parameters with the remote IPSec gateway
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
!
! Finally, a crypto-map that will be used to establish IPSec tunnels is applied to the physical interface
interface FastEthernet4/0
 ip address 10.0.0.2 255.0.0.0
```

```
 crypto map IOS_IOS
!
! The mirror ACL will trigger the IPSec tunnel establishment
access-list 151 permit ip host 192.168.1.2 host 192.168.2.1 log
end
```

### Cisco PIX: exemple de configuration

Voici un exemple de tunnel IPSec ESP-HMAC-SHA ESP-NULL configuré sur Cisco PIX.

```
PIX Version 6.2(1)
hostname pix
domain-name domain.top
!
****
!
! The following ACL will be used to trigger the IPSec tunnel establishment
access-list 101 permit ip host 192.168.3.1 host 192.168.1.2

! IPSec protocol must be enabled in the device
sysopt connection permit-ipsec
no sysopt route dnat

! "transform-set" command defines which kind of IPSec tunnel it will be possible to establish
crypto ipsec transform-set MoreSecure2 esp-null esp-sha-hmac

! A crypto map defines the IPSec parameters, which will be negotiated during the IPSec tunnel establishment
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

! The isakmp (ike) policy parameters are used when the device tries to establish the IKE tunnel
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.1 Exemple de configuration avec FreeS/WAN

Voici le fichier de configuration (ipsec.conf) de FreeS/WAN pour la configuration ESP-HMAC-SHA ESP-3DES.

```
# /etc/ipsec.conf - FreeS/WAN IPsec configuration file

# More elaborate and more varied sample configurations can be found
# in FreeS/WAN's doc/examples file, and in the HTML documentation.

# basic configuration
config setup
        # THIS SETTING MUST BE CORRECT or almost nothing will work;
        # %defaultroute is okay for most simple cases.
        interfaces=%defaultroute
        # Debug-logging controls:  "none" for (almost) none, "all" for lots.
        klipsdebug=none
        plutodebug=all
        # Use auto= parameters in conn descriptions to control startup actions.
        plutoload=%search
        plutostart=%search
        # Close down old connection when new one using same ID shows up.
        uniqueids=yes

# defaults for subsequent connection descriptions
conn %default
        # How persistent to be in (re)keying negotiations (0 means very).
        keyingtries=2
        # RSA authentication with keys from DNS.
        # authby=secret
        authby=rsasig
        #
        # use x509 certificates
        #
        leftrsasigkey=%cert
        rightrsasigkey=%cert
```

```
        #
        #freeswan security gateway
        left=192.168.1.20
        leftsubnet=192.168.1.20/32
        leftid=@host.domain.top
        #
        keyexchange=ike


# the following is the IPSec configuration towards the "cisco" router

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
```

# Annexe B - Références


- *A cryptographic Evaluation of IPSec* - Niels Ferguson et 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
- IPSec Protocol : http://www.ietf.org/html.charters/ipsec-charter.html
- IPSec RFCs - http://www.ietf.org/rfc.html
- *IPSec Securing VPNs* - Carlton R. Davis - RSA Press
- VPN Consortium : http://www.vpnc.org

# Annexe C - Liste des abréviations utilisées dans le présent document

| | |
|---|---|
| 3DES | Standard de chiffrement *(Triple Data Encryption Standard)* |
| AC | Autorité de certification |
| AES | Standard de chiffrement *(Advanced Encryption Standard)* |
| AH | Protocole d'authentification *(Authentification Header)* |
| CEPMMT | Centre européen pour les prévisions météorologiques à moyen terme |
| DES | Standard de chiffrement *(Data Encryption Standard)* |
| DH | Protocole de chiffrement à clé publique Diffie-Hellman *(Diffie-Hellman Key Agreement)* |
| DMZ | Zone « démilitarisée » |
| DWD | Service météorologique allemand |
| ESP | Protocole de confidentialité *(Encapsulating Security Payload)* |
| HMAC | Algorithme de chiffrement avec fonction de hachage *(Hashed Message Authentication Code)* |
| HNMS | Service météorologique grec |
| IKE | Protocole d'échange de clé *(Internet Key Exchange)* |
| IPSec | Protocole de sécurité pour IP *(IP Security Protocol)* |
| KNMI | Service météorologique néerlandais |
| LCR | Liste des certificats révoqués |
| MD5 | Algorithme de chiffrement à condense de message *(Message Digest 5)* |
| NAT | Traduction (on voit le plus souvent translation) d'adresses réseau *(Network Address Translation)* |
| RFC | Demande de commentaires – publication de référence portant sur le réseau Internet *(Request For Comments)* |
| RNIS | Réseau numérique à intégration de services |
| RPV | Réseau privé virtuel |
| RRTDM | Réseau régional de transmission de données météorologiques |
| RSA | Algorithme RSA *(Rivest, Shamir, Adleman)* |
| SHA | Algorithme de chiffrement irreversible *(Secure Hash Algorithm)* |
| UDP | Protocole *(User Datagram Protocol)* |
| URL | Adresse Web *(Universal resource locator)* |