TECHNICAL NOTES

IPSec Feasibility Study (in cooperation with DWD, Météo France, HNMS and KNMI):

Summary and recommendations

Network and Security Section
Computer Division
May 2003

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

European Centre for Medium-Range Weather Forecasts
Shinfield Park, Reading, Berkshire RG2 9AX, England

Contents

1 Introduction

During 2002 ECMWF and four Member States (Germany, Greece, France and the Netherlands) undertook IPSec tests in order to evaluate the feasibility of using an IPSec-based VPN as a back up for the RMDCN and for the transfer of amounts of data, which are excessive relative to the capacity of the RMDCN.

As most RMDCN sites have Internet access, using an IPSec-based VPN link as an additional backup, in case of a failure of the RMDCN link and its associated ISDN backup, will help to guarantee service continuity.

The RMDCN is a purpose-built network for real-time and operational data transfer and the various allocated bandwidths have a limited throughput. The Internet can be used in addition to the RMDCN to perform data transfer for cases where the RMDCN capacity is insufficient. However, it is worth keeping in mind that:

- The Internet lacks the concept of guaranteed bandwidth and QoS (Quality of Service) and is subject to various attacks, including DoS (Denial of Service) attacks.
- Long lasting outages occur on the Internet from time to time

This document reports on the results of the IPSec tests and provides guidelines and recommendations for building secure connections over the Internet. It is divided into four parts:

Part 1 gives a brief introduction to Virtual Private Networks and IPSec.
Part 2 describes the IPSec tests that were carried out.
Part 3 presents the results of the tests.
Part 4 details the recommendations.

2 Technical Overview

2.1 IP VPN definition

A Virtual Private Network is a group of two or more computer systems connected "securely" over a public network. VPNs can be installed between an individual machine and a private network (remote user-to-site) or between private networks (site-to-site). Security features differ from product to product, but most security experts agree that VPNs should include encryption, strong authentication of remote users or hosts, and mechanisms for hiding or masking information about the private network topology from potential attackers on the public network.

2.2 IPSec protocol

IPSec is an end-to-end security protocol: all the functionality and intelligence of the VPN connection reside at the end points, either in a gateway or in the end-host.

The service provider's IP network is not aware of the existence of the IP VPN, as tunnelling technologies ensure the transport of application data by encapsulation. The source address and the destination address of these packets are the IP addresses of the end points of the tunnel. They are then routed as any normal IP packets through the shared IP network.

In the past, several IP tunnelling protocols have been deployed. Over the last 3 years, however, IPSec has become the predominant IP tunnelling protocol and is currently the technology of choice when implementing site-to-site connectivity over a public network. IPSec was initially developed to ensure private communications over public IP networks. The protocol supports two main security functions:

- Authentication: ensuring the authenticity and the integrity of the whole IP packet;
- Encryption: ensuring the confidentiality of the payload.

Through IPSec it is possible to define a tunnel between two gateways. An IPSec gateway would typically be an access router or a firewall on which the IPSec protocol is implemented. IPSec gateways sit between the user's private network and the carrier's shared network.

IPSec tunnels are established dynamically and released when they are not in use. To establish an IPSec tunnel, two gateways must authenticate themselves and define which security algorithms and keys they will use for the tunnel. The entire original IP packet is encrypted and wrapped inside IPSec authentication and encryption headers. This becomes the payload of a new IP packet whose source and destination IP addresses are the public network IP addresses of the IPSec gateways. This ensures the logical separation between VPN traffic flows in a shared IP network. Traditional IP routing is then used between the tunnel end points.

IPSec achieves these objectives by using:

- Two traffic security protocols: the Authentication Header (AH), which provides data integrity, and the Encapsulation Security Payload (ESP), which provides data integrity and data confidentiality.
- A cryptographic-key management protocol: the Internet Key Exchange (IKE), which is used to negotiate IPSec connections.

For further information about IPSec protocol, see the list of References in Annex B.

3 The IPSec Tests

The main goals of these tests were:

- **Evaluate the feasibility of using IPSec tunnels to establish site-to-site connectivity:** Although several documents have been written regarding the implementation of IPSec and its various issues, it was worth testing it, in order to gain a thorough understanding of the IPSec protocol itself, to have an appreciation of its complexity and to evaluate the feasibility of its implementation in the context of the RMDCN.
- **Test the interoperability of IPSec :** The meteorological centres connected to the RMDCN may already have some equipment (router, firewall, etc.), which is IPSEC capable. Even if interoperability will not be an issue today, the interoperability of different devices has to be checked.
- **Define global recommendations:** RMDCN sites that are considering implementations of IPSec can use this document and its recommendations as a starting point.

3.1 IPSec parameter settings

As it was not feasible to test all IPSec features and capabilities, the tests focused on a subset. An initial option was chosen for each IPSec parameter:

Tunnel mode vs. Transport mode

Both AH and ESP protocols operate in two modes: transport mode and tunnel mode. Each of these modes has its wn applications:

- Tunnel mode is commonly used to encrypt traffic between secure IPSec gateways.
- Transport mode is used between end stations supporting IPSec or between an end station and a gateway, if the gateway is regarded as a host.

As the aim of the tests was to investigate secure site-to-site connections, only *IPSec "Tunnel mode" was considered* (see Figure 1 below) in the framework of this study.

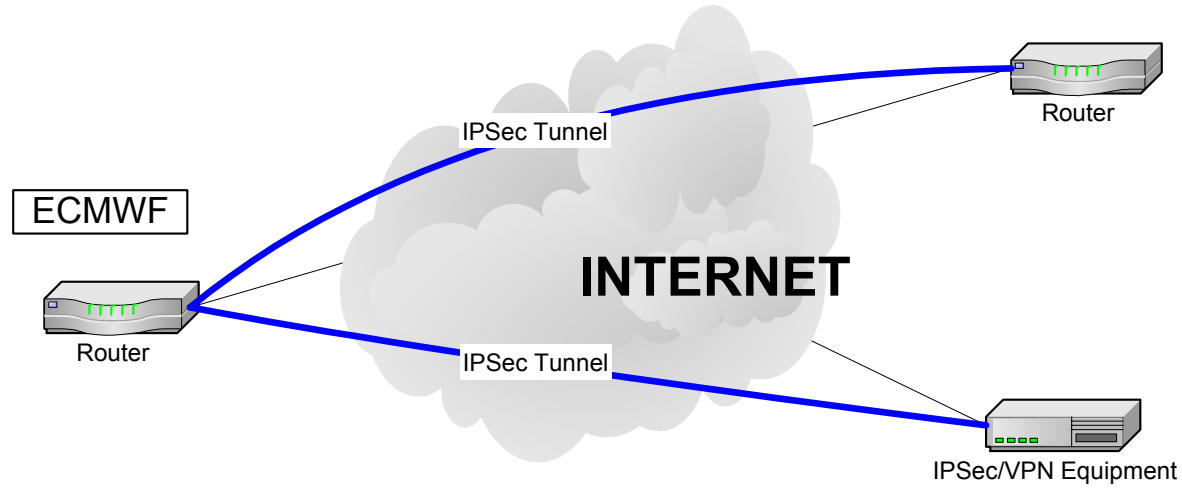

Figure 1 - IPSec "Tunnel mode" tests

Key exchange

IPSec Tunnel keys can be managed either manually or dynamically. For scalability and maintainability reasons, *IKE was used for the dynamic key management* during the tests.

Device authentication method

The IKE protocol is very flexible and supports multiple authentication methods. The two peers must agree on a common authentication method through a negotiation process. The two main authentication protocols are:

- **PreShared key:**
  The same key is configured on each IPSec peer. IKE peers authenticate each other by computing and sending a keyed hash of data using the configured PreShared key. If the receiving peer is able to create the same hash independently using its own PreShared key, it knows that both peers must share the same secret, thus authenticating the other peer.
- **RSA (Rivest, Shamir, Adleman) Signature:**
  This uses a digital signature, where each device digitally signs a set of data and sends it to the other party. RSA signatures use a CA (Certificate Authority) to generate a unique digital certificate that is assigned to each peer for authentication. The digital certificate is similar in function to the PreShared key, but provides much stronger security.

PreShared keys are easy to implement but do not scale well, as each IPSec peer must be configured with the PreShared key of every other peer with which it will establish a session. In addition, PreShared keys are less secures and are configured in clear text format in some equipment, for example in a Cisco router.

Therefore*, RSA signatures using x509 v.3 certificates were used*.

Data integrity and authenticity

Data integrity is implemented by including a message digest (or fingerprint) of the data within the IPSec packets. Message digests are calculated using hash functions. All IPSec capable devices should support hash functions HMAC-MD5 and HMAC-SHA, as stated in the RFC (Request For Comments) 2401. Therefore, other less commonly used hash functions were ignored. HMAC-MD5 and HMAC-SHA are based on MD5 and SHA combined with the additional crypto features of the HMAC algorithm. This is done to avoid tampering with the message digest itself. MD5 produces a 128-bit message digest and SHA produces a 160-bit message digest, therefore SHA is a more secure hash function than MD5. However, the HMAC-SHA and HMAC-MD5 variants used are truncated to the most significant 96 bits. Truncation has security advantages (less information on the hash available to the attacker) and disadvantages (less bits to predict for the attacker). In our opinion both truncated versions of HMAC-SHA and HMAC-MD5 are secure enough for our requirements.

In our test environment, *both HMAC-SHA and HMAC-MD5 were used; there was a slight preference for HMAC-SHA*.

Data encryption

Data confidentiality is achieved in IPSec by the use of symmetric encryption algorithms and session keys. The most commonly used algorithms are:

- ESP-NULL: No encryption applied.
- DES (Data Encryption Standard): Provides encryption using a 56 bit key.
- 3DES (Triple Data Encryption Standard): Provides encryption using a 168 bit key.
- AES (Advanced Encryption Standard): Provides encryption using 128, 192, and 256 key lengths.

According to RFC 2401, all IPSec devices should support at least ESP-NULL and DES. However, DES is considered a weak encryption algorithm due to its short key length, and as such, some vendors discourage its use and some others refuse to support it (i.e. FreeS/Wan).
Therefore, for the purpose of this test, *NULL (no encryption) and 3DES encryption were used whenever possible*. DES was only used when 3DES was not available.

An international VPN/IPSec via Internet must comply with the legislation of each country (encryption, size of the key…). Therefore, each site should be aware of national policy before using encryption.

Session key exchange

Diffie-Hellman (DH) is a public-key cryptography protocol. It allows two parties to establish a shared secret between them. DH is used within IKE to establish a shared secret that is used as a session key. The most common DH groups are:

- Group 1: Uses a 768 bit public key to establish a shared secret.
- Group 2: Uses a 1024 bit public key to establish a shared secret.

For the purpose of the tests, *DH Group 2 was used* since it is more secure and does not create any overhead for the IPSec devices.

3.2 The lab tests

In order to validate the selected parameter settings of the IPSec features and before performing any external (through the Internet) tests, a test environment was set up at ECMWF to conduct some preliminary experiments. The aim of these tests was to get familiarised with IPSec configuration and the certificate enrolment process.

Figure 2 shows the configuration of the test environment.

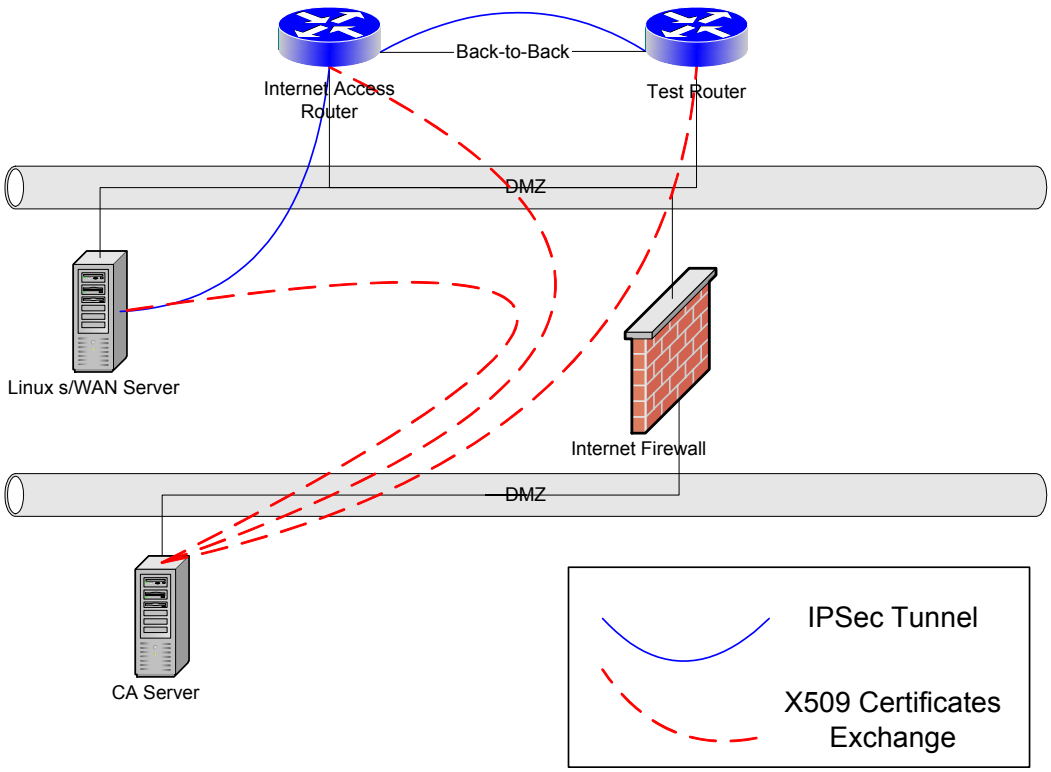

Figure 2 - Network configuration test environment

With this setup, we were able to:

- Test three different authentication methods: PreShared keys, public encryption (RSA_ENCR) and public keys signed by a Certification Authority (RSA_SIG).
- Test X509 certification enrolment and utilisation.
- Perform basic IPSec configuration: build tunnels with the chosen IKE/IPSec parameters.
- Test a public domain IPSec implementation: FreeS/WAN
- Test IPSec interoperability between several devices.

The test environment was also used during the Internet tests to reproduce problems in order to fix them.

3.3 Internet tests

Figure 3 shows an overall view of the IPSec tests performed across the public Internet. The objective of these Internet tests was to build secure connections between ECMWF and the Member States and use them to transfer data. Configuration examples can be found in Annex A.

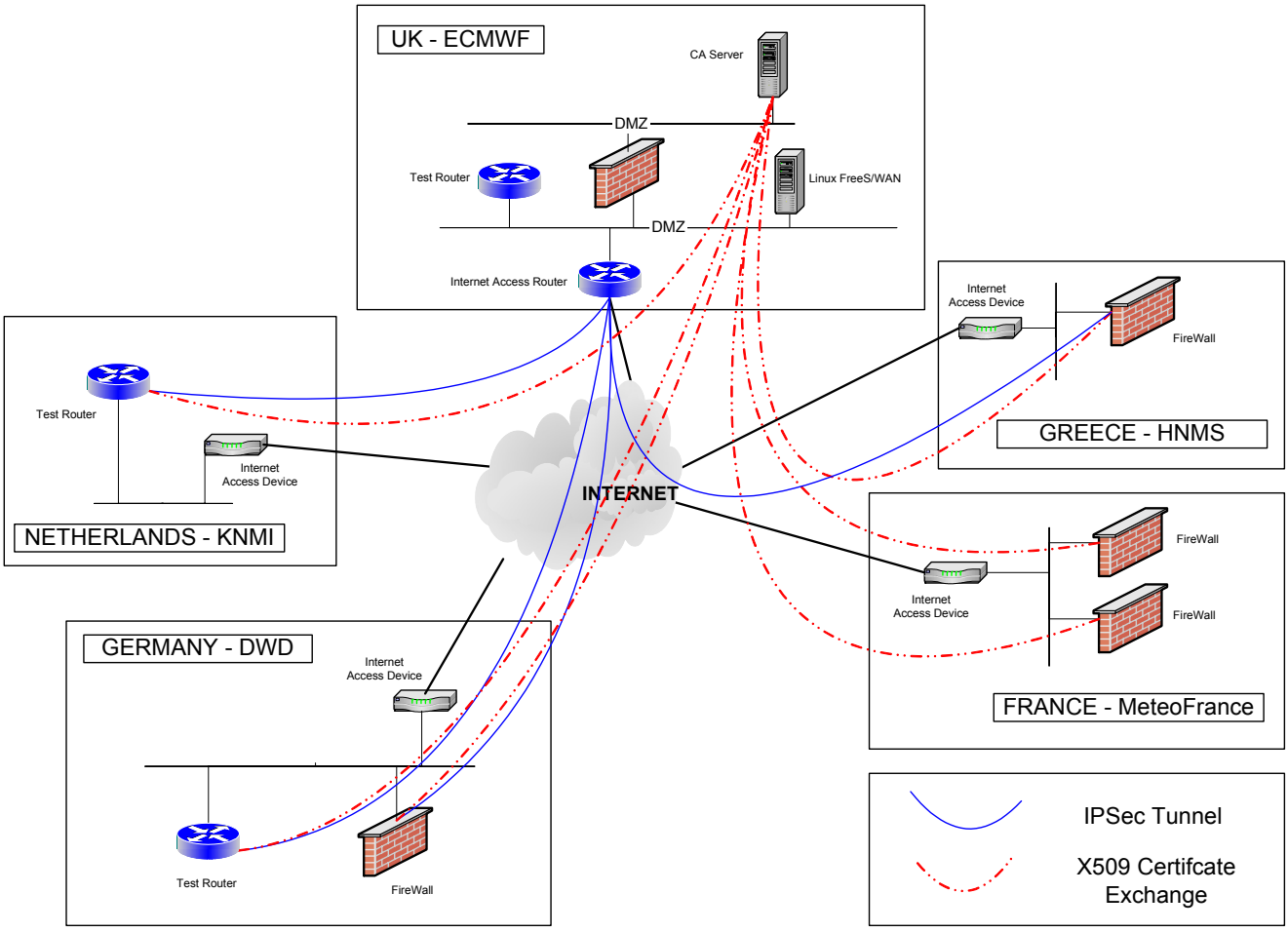

Figure 4 - Network configuration for the Internet tests

4 Test Results

The following sections briefly describe the four tests conducted with the Member States and highlight some of the experiences.

4.1 Test #1: Certificate enrolment and device authentication

The purpose of this test was to see how the different devices would go through the certificate enrolment process and use the X509 certificate for device authentication. If there were problems with devices using X509 certificates, PreShared keys were configured manually in the device. Most of the tested devices succeeded in enrolling and using certificates for authentication[1].
The main issues encountered during this test were due to the fact that the devices use different certificate enrolment methods (mainly URL and "out-of-band" download) and diverse certificate formats.

4.2 Test #2: Data Integrity

The purpose of this test was to establish basic IPSec connections using HMAC (SHA and MD5) algorithm to check the data integrity. The IKE negotiation used the X509 certificate downloaded from the CA server. Except for FreeS/WAN, which does not implement the AH protocol, all the tested devices were able to establish AH and ESP HMAC IPSec tunnels.

4.3 Test #3: Data Encryption

This test is a follow-up of test #2; it adds 3DES encryption. When 3DES was not available, DES was used. The tests were carried out successfully. However, it is important to take into account that 3DES/DES encryption capability depends on the device hardware and software versions.

4.4 Test #4: Performance tests

In order to evaluate the impact of IPSec tunnelling on the CPU, a set of FTP tests was undertaken. Several FTP tests were carried out, both with and without the establishment of IPSec tunnels.
The configuration below (Figure 5) was used to conduct the FTP tests; router B represents a generic remote router that guarantees the Internet connection to and from a Member State.

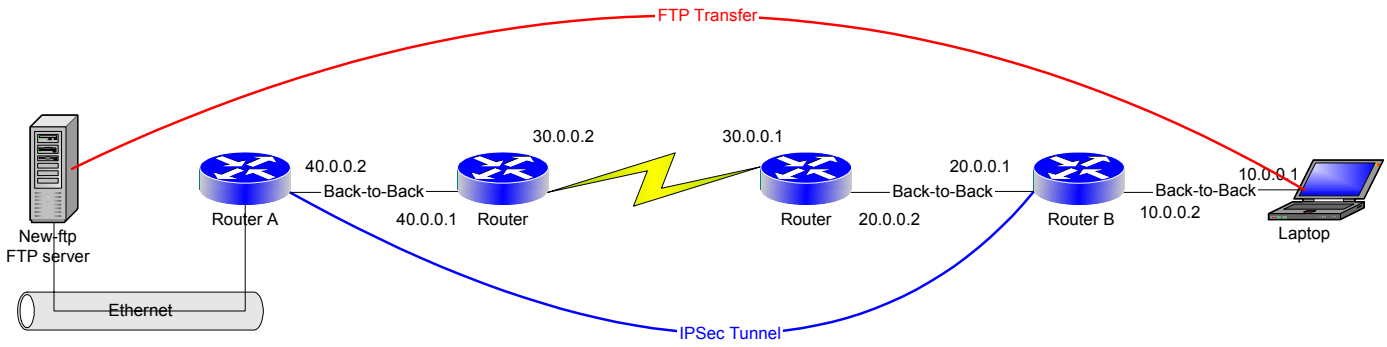

Figure 5 - FTP Tests Lab Setup

[1] CheckPoint FW1 equipment: only the enrolment of the certificate was tested. FW1 requires a Control Revocation List (CRL) to start the IPSec process. The use of CRLs was not included in the tests. This will be done at a future stage.

Tests were also conducted across the Internet between ECMWF and a Cisco PIX firewall at DWD in Germany.

The main conclusions from the performance tests are:

- IPSec protocol has a significant impact on the CPU load of the device.
- Encrypted tunnels are more CPU consuming than non-encrypted ones.
- HMAC-MD5 algorithm is slightly less CPU consuming than HMAC-SHA algorithm.
- ESP protocol for data integrity is equally as CPU consuming as AH protocol.
- A small IPSec capable router (such as a Cisco 1605) is not suitable for IPSec tunnelling when the Internet connection speed is higher than 128 kb/s.

5 Recommendations

The following recommendations are based on the results of the tests described in section 3. These recommendations should help sites to build secure IPSec connections over the public Internet.

5.1 Device authentication

The use of X509 certificates for device authentication is recommended for the following reasons:

- It is the most secure method.
- It is the most scalable method.

Furthermore, the generation of 1024 bit RSA keys and the use of DH group 2 (encryption algorithm) are recommended.

5.2 Data integrity

Both AH and ESP protocols can be used for packet authentication. However:

- The tests showed that ESP consumes as much CPU load as AH.
- Only ESP protocol can ensure packet encryption (see Section 4.3).

Therefore, for reasons of simplicity the use of ESP HMAC for packet authentication is recommended. Also, either ESP-HMAC-MD5 or ESP-HMAC-SHA can be used.

5.3 Data encryption

Because of the nature of the data (meteorological) encryption is not strictly required. Since data encryption is CPU consuming ensuring packet authentication provides enough security. Therefore, the use of ESP NULL is recommended. This means that ESP will be applied to the packet with no encryption.
If ever data encryption is needed, the implementation of ESP-3DES is recommended, as it is more secure than DES.

5.4 The IPSec capable equipment

In the light of the previous recommendations (Sections 4-1 to 4-3), the following should be considered, when selecting an IPSec-capable device to implement a VPN:

- For scalability reasons, the device should be IKE capable and should support X509 certificate standard.
- It is important that the device supports ESP_NULL encryption method.
- If considering data encryption, the equipment must be 3DES-capable. Moreover, it should be taken into account that AES may soon become the de facto encryption standard. Therefore, equipment that is also AES-capable is desirable, in order to anticipate future requirements.
- For sites with a high speed Internet connection, a dedicated VPN/IPSec device with encryption card (acceleration card) is recommended, as it significantly reduces the CPU load when the IPSec protocol is used.

As a final note, the tests showed that it is easier to configure IPSec-capable equipment than to implement a public domain solution. Nevertheless, an open source implementation, FreeS/WAN, could be considered, bearing in mind that FreeS/WAN implements 3DES encryption by default (refer to http://www.freeswan.org for further details).

5.5 Network Design

When designing an IPSec implementation, a set of guidelines has to be taken into account. The VPN gateway should always be in a DMZ and never inside the "private" network. This means that the VPN device has to be somewhere between a Firewall and the external network (the Internet); all the traffic between the VPN device and the private internal network should go through a Firewall, see Figure 6. Because the VPN device is located on a DMZ, it is important to configure the Firewall to allow IPSec traffic to and from it. The following table shows the IP protocols and TCP/UDP port numbers a Firewall has to allow for IPSec to work:

Protocol/Port	**Comment:**
IP protocol 50	ESP protocol
IP Protocol 51	AH protocol
UDP 500	IKE negotiation
UDP/TCP 10000	NAT tunnelling

To implement IPSec, it is not mandatory to use a dedicated IPSec device. It is possible to combine IPSec and firewall capabilities or IPSec and Internet access capabilities or all three capabilities in a single device.

The following diagram (Figure 6) shows a topology on which a dedicated VPN/IPSec device is used in addition to the Internet access router and the Firewall.

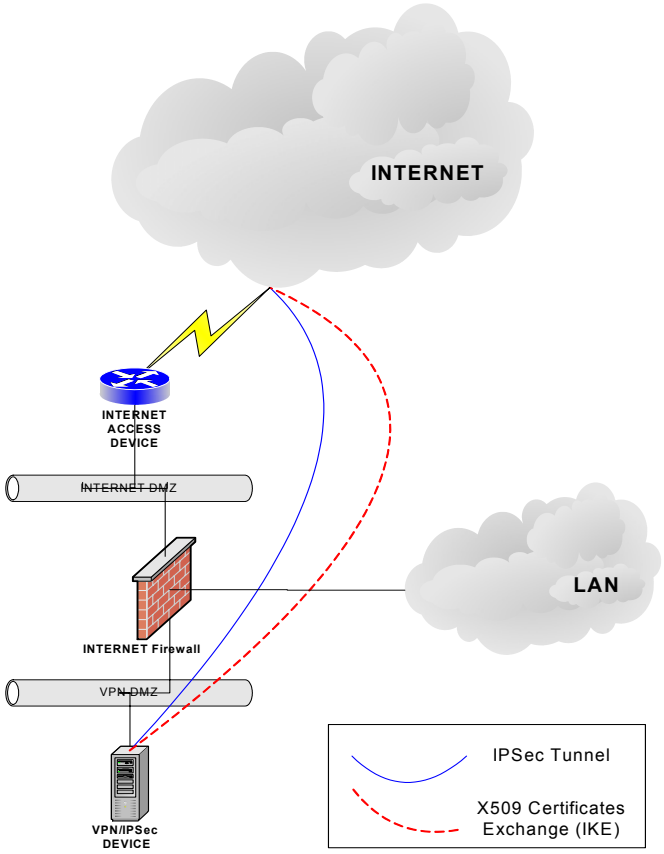

Figure 6 - VPN Network Design using a dedicated VPN device

6 Acknowledgement

The following persons contributed to the study and the creation of this document:

Inge Essid, DWD
Ilona Glaser, DWD
Erwan Favennec, Meteo 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

Annex A - Configuration guidelines and examples

A.1 Output and configuration files for Cisco Router and PIX

Cisco IOS: certificate enrolment guideline

The main points to consider when requesting a certificate from a Cisco Router are:

1- Configure the Router's Host Name and Domain Name: Use “hostname” and “ip domain-name” global configuration commands.
2- Set the Router's Time and Date: ensure that the router's time zone, time and date have been accurately configured with the “set clock” command. The clock must be set before generating RSA key pairs and enrolling the certificate, as the keys and certificates are time-sensitive.
3- RSA key pairs must be generated using a modulus of 1024: using the “crypto key generate rsa” command, generate RSA key pairs with a modulus of 1024.
4- Declare the CA and configure its parameters:
   - To declare the CA: “crypto ca identity <CA identity>”
   - To configure its parameters: “enrolment url <CA server URL>” and “crl optional”
   - To authenticate the CA: “ca authenticate <CA identity>”
5- Request a X509 certificate: when requesting a X509 certificate, answer “no” when asked if you want to include:
   - The router serial number
   - An IP address in the subject name

Cisco IOS: enrolment output

The following is the output from a certificate enrolment performed on a Cisco router:

```
! 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: IPSec configuration example

The following is an ESP-HMAC-SHA ESP-NULL IPSec tunnel configuration example:

```
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: configuration example

The following is a ESP-HMAC-SHA ESP-NULL IPSec tunnel configuration example for a 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.2 FreeS/WAN configuration example

FreeS/WAN (ipsec.conf) configuration file for an ESP-HMAC-SHA ESP-3DES configuration example:

```
# /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
```

Annex B - References

- 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
- 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

Annex C - List of acronyms

3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
AH	Authentification Header
CA	Certificate Authority
CRL	Certificate Revocation List
DER	Distinguished Encoding Rules
DES	Data Encryption Standard
DH	Diffie-Hellman Key Agreement
DWD	Deutscher Wetterdienst
ECMWF	European Centre for Medium-Range Weather Forecasts
ESP	Encapsulating Security Payload
HMAC	Hashed Message Authentication Code
HNMS	Hellenic National Meteorological Service
IKE	Internet Key Exchange
IPSec	IP Security Protocol
KNMI	Koninklijk Nederlands Meteorologisch Instituut
MD5	Message Digest 5
NAT	Network Address Translation
PEM	Privacy Enhanced Mail
PKI	Public Key Infrastructure
QoS	Quality Of Service
RFC	Request For Comments
RMDCN	Regional Meteorological Data Communication Network
RSA	Rivest, Shamir, Adleman
SHA	Secure Hash Algorithm