NICC ND 1628 V 1.1.2 (2008-08)

NICC Document

SECURING DATA FLOWS WITH IPSEC FOR NGN INTERCONNECTS

Network Interoperability Consultative Committee,
Ofcom,
2a Southwark Bridge Road,
London,
SE1 9HA.

If you have any comments concerning the accuracy of the contents of this document, please write to:

The Technical Secretary,
Network Interoperability Consultative Committee,
Ofcom,
2a Southwark Bridge Road,
London SE1 9HA.

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to NICC.

Pursuant to the NICC IPR Policy, no investigation, including IPR searches, has been carried out by NICC. No guarantee can be given as to the existence of other IPRs which are, or may be, or may become, essential to the present document.

Foreword

This NICC Document (ND) has been produced by the NICC security working group.

1 Scope

The present document describes the use of IPsec to protect traffic across a connecting link between NGNs.

This profile is designed to support the purple and green release specifications but may be considered for use in other scenarios.

2 References

For the particular version of a document applicable to this release see ND1610 [5]

2.1 Informative references

[1] RFC 2409: “The Internet Key Exchange”

[2] RFCs 2401-11: IPSec specification documents

[3] RFC 4301: “Security Architecture for the Internet Protocol”

[4] RFC 3706: “A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers”

[5] ND1610 Multi-Service Interconnect of UK Next Generation Networks

3 Abbreviations

Null

4 Purpose

Other documents describe when information should be considered for protection with IPsec. As defined in the IETF standards RFCs 2401-11, IPsec provides cryptographic services for protecting the authenticity and confidentiality of transmitted data. Encryption is used to protect confidentiality; authentication is used to protect integrity. IPsec does not provide availability protection.

4.1 IKEv2

The NICC security working group recognises that IKEv2 has been standardised as part of the RFC 4301 series of IPsec specifications. However, IKEv2 is not interoperable with IKEv1 and many more devices support IKEv1. So, for the time being, the pragmatic approach is to support IKEv1.

As implementations of the new version of IPsec become more common this guidance is likely to evolve into a requirement to support IKEv2 and its companion protocols as described in RFC4301 and references therein.

5 IPsec configuration

5.1 Overview

Services **should** specify this profile of IPsec for data flowing across NGN interconnects where data privacy or authentication is required. This is in line with best practice from ETSI and vendor recommendations.

Where a CP has a requirement to examine the signalling at a high level to determine that it is legitimate it will be necessary to intercept the data in an unprotected form or, where IPsec integrity protection is used, to examine the contents of the ESP protected packets.

5.2 Policy

The following parameters are the main features of an IPsec policy and are required to enable IPsec peers to communicate. The parameters are fully described in RFC2401. See section 4.1 for the complete list of parameters that need to be manually exchanged.

- The IKE encryption algorithm: either 3DES-CBC or AES-CBC **may** be used. The key length **must** be at least 128-bits.
- The IKE mode: main mode **shall** be used.
- The IKE Security Association lifetime: 12 hours **shall be** used by default; other lifetimes **may** be used by mutual agreement.

  Note: The NICC security working group recommends that the IKE lifetime should be several times the length of the IPsec Security Association lifetime.
- Perfect Forward Secrecy: PFS **should** be enabled. Group 2 **should** be used by default. In this case, the Diffie-Hellman group used in the PFS enabled key exchange **shall** have a cryptographic strength equivalent to an RSA key of at least 1024 bits in length. Practically, this requirement means that any DH group apart from group 1 **may** be used.
- The IPsec encryption algorithm: either 3DES-CBC or AES-CBC **may** be used. The key length **must** be at least 128-bits.**Error! Bookmark not defined.** NULL encryption **must not** be used across interconnections.
- The IPsec authentication algorithm: the ESP protocol provides IPsec authentication. HMAC-SHA1-96 **should** be used to provide authentication. HMAC-MD5-96 **shall be** used where HMAC-SHA1-96 is unavailable.
- The IPsec Security Association lifetime: the lifetime **should** be explicitly specified as 1 hour.

  Note: The IPsec specifications provide for the IPsec SA to have a lifetime measured either in terms of time or in terms of the amount of data that has flowed under the SA. Given the likely level of signalling traffic on an interconnection, the NICC security working group recommends that time is used.
- Dead Peer Detection, as described in RFC 3706, **should** be used to keep IPsec protected peering connections alive in the absence of data traffic.

Where authentication is used, encryption **should** also be used. This is true even when protection of integrity is considered the most important security goal because: Encryption of the signalling actually prevents individual media streams being identified readily, thus providing enhanced media protection even through the media may be in the clear. It also adds protection against traffic analysis.

6. Waiving the IPsec requirement

IPsec **shall** be used to protect the data except where:

- Interconnecting communications providers agree to waive this requirement based on mutually agreed and documented security controls protecting the interconnecting infrastructure; and
- Those controls can be shown to deliver risk mitigation equal to or greater to that of the IPSec solution.

7. Management of IPsec interconnections

The management of IPsec interconnections can be divided into two distinct phases:

- Setting the interconnection up initially; and
- Ongoing management as it is used: this is the function of the key management protocol, which **shall** be IKEv1, as defined in RFC 2409.

Setting the connection up requires the exchange of certain information between the interconnecting CPs. This information **must** include at least the information in the table on section 7.1.

7.1 Manually exchanged information

* shows the default or recommended option

Parameter	**Options**	**Notes**
IPsec identification payload	*IP address: __ Other: __	
Shared secret	A randomly chosen alphanumeric password should be used.	The shared secret may be shared out of band or via encrypted e-mail and should be stored securely. Consider security carefully if sharing it via telephone, especially over the VoIP interconnect!
The IKE encryption algorithm	3DES-CBC *AES-CBC	The key length **must** be at least 128 bits.
The IKE mode	*Main mode	
The IKE security association lifetime	*12 hours	The IKE lifetime should be several times the length of the IPsec Security Association lifetime.
Perfect forward secrecy	Enabled	
Perfect forward secrecy group	*PFS DH group 2 PFS DH group 5	DH group 1 **shall not** be used, it is cryptographically weak.
The IPsec encryption algorithm	3DES-CBC *AES-CBC	The key length **must** be at least 128-bits.
The IPsec authentication algorithm	*HMAC-SHA1-96 HMAC-MD5-96	HMAC-SHA1-96 **should** be used to provide authentication. HMAC-MD5-96 **should be** used where HMAC-SHA1-96 is unavailable.
The IPsec security association lifetime	*1 hour	The lifetime should be determined by expiry time rather than data volume.
Dead peer detection	*Yes No	DPD described in RFC 3706, **may** be used to keep IPsec protected peering connections alive in the absence of data traffic.

Annex A (informative): Other uses of this specification

The network inside a CP's domain is outside the scope of this specification.

However, the NICC security working group recommends that IPsec protection should be used within the CP's domain. In this case it may more appropriate to use IPsec with data authentication alone.

In these circumstances NULL encryption may be considered.

History

Document history		
<Version>	<Date>	<Milestone>
V1.1.1	April 2008	Initial issue