PANA Working Group
Internet Draft
Document: draft-ietf-pana-ipsec-07.txt
Expires: January 2006

M. Parthasarathy
Nokia

July 2005

# PANA Enabling IPsec based Access Control

## Status of this Memo



## Copyright Notice



## Abstract

PANA (Protocol for carrying Authentication for Network Access) is a protocol for authenticating clients to the access network using IP based protocols. The PANA protocol authenticates the client and also establishes a PANA security association between the PANA client and PANA authentication agent at the end of a successful authentication. This document discusses the details for establishing an IPsec security association using the PANA security association for enabling IPsec based access control.

## Table of Contents

## 1.0 Introduction

PANA (Protocol for carrying Authentication for Network Access) is a protocol [PANA-PROT] for authenticating clients to the access network using IP based protocols. The PANA protocol authenticates the client and also establishes a PANA security association between the PANA client (PaC) and PANA authentication agent (PAA) at the end of successful authentication. The PAA indicates the results of the authentication using the PANA-Bind-Request message wherein it can indicate the access control method enforced by the access network. The PANA protocol [PANA-PROT] does not discuss any details of IPsec [RFC2401] security association (SA) establishment, when IPsec is used for access control. This document discusses the details of establishing an IPsec security association between the PANA client and the enforcement point. The IPsec SA is established using IKE [RFC2409], which in turn uses the pre-shared key derived from the EAP authentication. The IPsec SA used to protect the packet provides the assurance that the packet comes from the client that authenticated to the network. Thus, the IPsec SA can be used for access control and specifically used to prevent the service theft mentioned in

[RFC4016]. The term "access control" in this document refers to the per-packet authentication provided by IPsec. IPsec is used to protect packets flowing between PaC and EP in both directions.

Please refer to [PANAREQ] for terminology and definitions of terms used in this document. The PANA framework document [PANA-FRAME]





describes the deployment scenarios for IPsec. The following picture illustrates what is being protected with IPsec. The different scenarios of PANA usage are described in the [PANAREQ]. When IPsec is used, scenarios 3 and 5 are supported as shown below. As shown in Figure 1, the Enforcement Point (EP), Access Router (AR) and the PANA authentication agent are co-located which is described as scenario 3 in [PANAREQ].

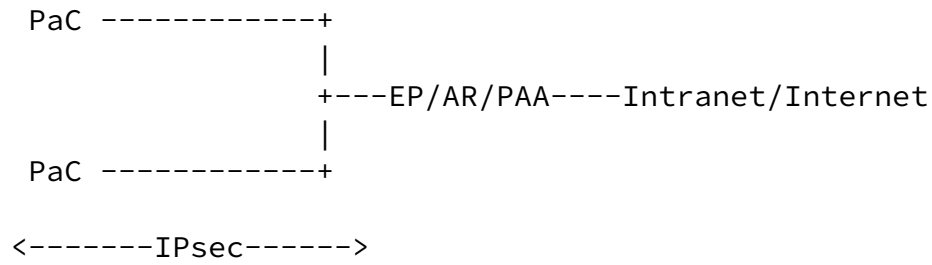


Figure 1: PAA/EP/AR are co-located

As show in Figure 2, only the AR and EP are co-located. The PAA is a separate node though located on the same link as the AR and EP. All of them are one IP hop away from the PaC. This is the same as scenario 5 described in [PANAREQ].

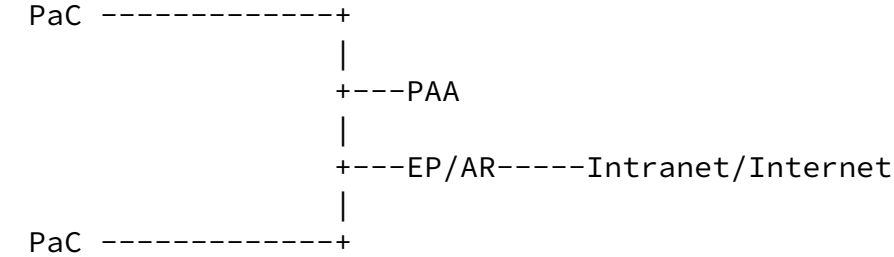


Figure 2: EP and AR are co-located

The IPsec security association protects the traffic between the PaC and EP. In IPsec terms, the EP is a security gateway (therefore a router) and forwards packets coming from the PaC to other nodes.

First, this document discusses some of the pre-requisites for IPsec SA establishment. Next, it gives details on what should be





communicated between the PAA and EP. Then, it gives the details of IKE exchange with IPsec packet formats and SPD entries. Finally, it discusses the dual stack operation.

## 2.0 Keywords

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2118].

## 3.0 Pre-requisites for IPsec SA establishment

This document assumes that the following have already happened before the IKE exchange starts.

1) The PaC) and PAA mutually authenticate each other using an EAP method that is able to derive a AAA-key [EAP-KEY].

2) The PaC learns the IP address of the Enforcement point (EP) during the PANA exchange.

3) The PaC learns that the network uses IPsec [RFC2401] for securing the link between the PaC and EP during the PANA exchange.

## 4.0 IP Address Configuration

The IP address configuration is explained in [PANA-FRAME]. Some of the details relevant to IPsec are briefly repeated here for clarity.

The PaC configures an IP address before the PANA protocol exchange begins. This address is called a pre-PANA address (PRPA). After a successful authentication, the client may have to configure a post-PANA address (POPA) for communication with other nodes, if PRPA is a local-use (e.g., link-local or private address) or a temporarily allocated IP address.

The PRPA of the PaC may be a link-local address [IPV4-LINK] or a private address [RFC1918] or a routable address or an IPv6 link-local address or global address [RFC2462]. Please refer to [PANA-FRAME] for more details on how these addresses may be configured. The PaC would use the PRPA as the outer address of IPsec tunnel mode SA (IPsec-TOA). The PaC also needs to configure an inner address (IPsec-TIA). There are different ways to configure IPsec-TIA.

1) Some IPv4 IPsec implementations are known to work properly when the same address is configured as both the IPsec-TIA and IPsec-TOA. When PRPA is a routable address, the PRPA may be used as both the IPsec-TIA and IPsec-TOA and POPA may not be configured.





2) In IPv4, an IPsec-TIA can be obtained via the configuration method available using DHCP over IPsec tunnels [RFC3456]. The minor difference from the original usage of [RFC3456] is that the IPsec-TOA does not need to be a routable address when [RFC3456] is used between the PaC and EP.

3) When IKEv2 [IKEV2] is used for security association negotiation, the address configuration method available in [IKEV2] can be used for configuring the IPsec-TIA for both IPv4 and IPv6.

There are other address configuration methods possible. They have some implementation issues, which are described in the Appendix A.

## 5.0 IKE Pre-shared key derivation

If the network chooses IPsec to secure the link between the PaC and EP, the PAA should communicate the IKE pre-shared key (Pac-EP Master Key), Key-Id, the device identifier of the PaC, and the session-Id to the EP before the IKE exchange begins. Whenever the IKE pre-shared key changes due to re-authentication as described below, the new value is computed by the PAA and communicated to the EP with all the other parameters.

The IKE exchange between the PaC and PAA is equivalent to the 4-way handshake in [IEEE80211i] following the EAP exchange. The IKE exchange establishes the IPsec SA similar to the pair-wise transient key (PTK) established in [IEEE80211i]. The IKE exchange provides both key confirmation and protected cipher-suite negotiation.

The IKE pre-shared key is derived as follows (where "|" means concactenation).

```
IKE Pre-shared Key = HMAC-SHA-1 (PaC-EP-Master-Key,
                          "IKE-preshared key" |
                          Session ID | Key-ID | EP-address)
```

The values have the following meaning:

PaC-EP-Master-Key: A key derived from the AAA-key for each EP as defined in [PANA-PROT].

Session ID: The value as defined in the PANA protocol [PANA-PROT], identifies a particular session of a client.

Key-ID: This identifies the PaC-EP-Master-Key within a given session [PANA-PROT]. During the lifetime of the PANA session, there could be multiple runs of EAP re-authentications. As EAP re-authentication changes the AAA-key which in turn affects Pac-EP-Master-Key, Key-ID





is used to identify the right PaC-EP-Master-Key. This is contained in the Key-ID AVP [PANA-PROT].

EP-address: This is the address of the enforcement point with which the IKE exchange is being performed. When the PAA is controlling multiple EPs, this provides a different pre-shared key for each of the EPs.

During EAP re-authentication, the AAA-Key changes. Whenever the AAA-Key changes, a new PaC-EP-Master-Key is derived and a new value for Key-ID is established between the PaC and PAA/EP as defined in [PANA-PROT]. The [EAP-KEY] document requires that all keys derived from AAA-key be deleted when the AAA-key expires. Hence, a new IKE PSK should be derived upon AAA-key expiry. As it also affects the IKE and IPsec SAs derived from it, new security associations for IKE and IPsec are established with the new IKE PSK. In case where two runs of EAP authentication (NAP/ISP) are performed during a single PANA authentication phase, a new PaC-EP-Master-Key is derived from the

AAA-key obtained from both authentications as specified in the [PANA-PROT].

## 6.0 IKE and IPsec details

IKE [RFC2409] MUST be used for establishing the IPsec SA. The details specified in this document works with IKEv2 [IKEV2] as well as IKE. Any difference between them would be explicitly noted. PANA authenticates the client and network, and derives the keys to protect the traffic. Hence, manual keying cannot be used. If IKE is used, aggressive mode with pre-shared key MUST be supported. The PaC and EP SHOULD use the following value in the payload of the ID_KEY_ID to identify the pre-shared key.

ID_KEY_ID data = (Session-Id | Key-Id)

The Session-Id and Key-Id are the values contained in the data portion of the Session-Id and Key-Id AVP respectively [PANA-PROT]. They are concatenated to form the content of ID_KEY_ID data. IP addresses cannot be used as identifier as the same PaC or different PaC may use the same IP address across a PANA session. For the same reason, main mode of IKE cannot be used, as it requires addresses to be used as identifiers.

If IKE is used, a quick mode exchange is performed to establish an ESP tunnel mode IPsec SA for protecting the traffic between the PaC and EP. In IKEv2, the initial exchange (IKE_SA_INIT and IKE_AUTH) creates the IPsec SA also. The identities (a.k.a. traffic selectors in IKEv2) used during Phase 2 are explained later along with the SPD entries. As mentioned in section 4.0, an address (POPA) may also have





to be configured. The address configuration method to be used by the PaC is indicated in the PANA-Bind-Request message at the end of the successful PANA authentication. The PaC chooses the appropriate method and replies back in PANA-Bind-Answer message.

## 7.0 Packet Formats

Following acronyms are used throughout this document.

PAC-TIA denotes the IPsec-TIA used by the PaC. PAC-TIA may be set to a PRPA when the same PRPA is used as the IPsec-TIA and IPsec-TOA on the PaC. Otherwise, PAC-TIA is set to the POPA.

PAC-TOA denotes the IPsec-TOA used by the PaC.

EP-ADDR denotes the address of the EP.

The node with which the PaC is communicating is denoted by END-ADDR.

Following is the IPv4 packet format on the wire for packets sent from the PaC to the EP:

```
      IPv4 header      (source = PAC-TOA,
                        destination = EP-ADDR)
      ESP  header
      IPv4 header      (source = PAC-TIA,
                        destination = END-ADDR)
```

Following is the IPv6 packet format on the wire for packets sent from the PaC to the EP:

```
      IPv6 header      (source = PAC-TOA,
                        destination = EP-ADDR)
      ESP  header
      IPv6 header      (source = PAC-TIA,
                        destination = END-ADDR)
```

Following is the IPv4 packet format on the wire for packets sent from the EP to the PaC:

```
      IPv4 header      (source = EP-ADDR,
                        destination = PAC-TOA)
      ESP  header
      IPv4 header      (source = END-ADDR,
                        destination = PAC-TIA)
```

Following is the IPv6 packet format on the wire for packets sent from the EP to the PaC:





```
      IPv6 header      (source = EP-ADDR,
                        destination = PAC-TOA)
      ESP  header
      IPv6 header      (source = END-ADDR,
                        destination = PAC-TIA)
```

## 8.0 IPsec SPD entries

The SPD entries for IPv4 and IPv6 are specified separately as they are different. When the same address is used as IPsec-TIA and IPsec-TOA, the EP can add the entry to the SPD before the IKE exchange starts, as it knows the address a priori. When IKEv2 [IKEV2] or [RFC3456] is used for address configuration, the SPD entry cannot be created until the IPsec SA is successfully negotiated as the address is not known a priori. This is very similar to the road warrior case described in [IPSEC-BIS]. In this case, an SPD entry with a name selector is used and when the IPsec SA is successfully negotiated, a new SPD entry is created with the appropriate addresses. The name would be the contents of ID_KEY_ID payload.

In environments where the PaC is a router, the IPsec-TIA can be a range of addresses (prefix) instead of a single host address. The PaC acts like a security gateway in this case establishing the IPsec SA with another security gateway (EP). This scenario is supported by [RFC2401] and [IPSEC-BIS]. It is assumed that the PaC obtains the prefix through other mechanisms not defined in this document. When the IPsec SA is negotiated, the prefix is carried in the traffic selectors.

Each SPD entry specifies packet disposition as BYPASS, DISCARD or PROTECT. The entry that causes the traffic to be protected with IPsec uses IPsec-TIA as the selector. This has the side effect of protecting all the traffic, which could be a problem. Some of the traffic that is not protected with IPsec is discussed below.

. The neighbor discovery messages specified in [RFC2461] are protected using [RFC3971]. The Multicast listener Discovery messages specified in [RFC2710] are also bypassed as IKE can negotiate keys only for unicast traffic. The SPD contains entry based on ICMPv6 type (130 to 137) to bypass such traffic.

. When IPsec-TIA and IPsec-TOA are the same (as discussed in section 4.0), the PANA traffic also gets protected with IPsec. As the IPsec protection adds extra overhead without any benefit, we need explicit entries to bypass IPsec protection for PANA traffic on PaC. This may not be needed always for traffic going from PAA to PaC. If PAA and EP are not co-located, PAA would send traffic directly to PaC without going through EP. Hence, EP does not need to have SPD entries to bypass IPsec in this case.

If PAA and EP are co-located, the PANA packets will be protected with IPsec only if the IPsec-TIA and IPsec-TOA are same. Hence, we need explicit entries to bypass IPsec protection when PAA and EP are co-located. The SPD entry is specified using PANA_PORT. PANA_PORT is the IANA assigned (TBD) PANA protocol number [PANA-PROT].

There may be protocols that expect the TTL to be 255, which may not be preserved as a result of IP forwarding by the EP. If the protocol termination is in a different place than EP, then we may need additional bypass entries for those protocols, which are not shown here. Also, when the PaC is using IPsec for remote access, there may be additional SPD entries and IPsec security associations, which are not discussed in this document.

The format chosen to represent the SPD rules is similar to the one used in [IPSEC-BIS] document (See Appendix E). Following acronyms are used.

Rule - SPD rule and this column has ordered rules.
LADDR - Local address
RADDR - Remote address
LPORT - Local Port
RPORT - Remote Port
ITYPE - Specifies ICMPv6 type
Action - Specifies the IPsec actions (BYPASS, DROP, PROTECT)

## 8.1 IPv4 SPD entries

PaC's SPD:

| Rule | LADDR | RADDR | LPORT | RPORT | Action |
|---|---|---|---|---|---|
| Rule 1 | ANY | PAA-ADDR | ANY | PANA_PORT | BYPASS |
| Rule 2 | PAC-TIA | ANY | ANY | ANY | PROTECT (ESP, tunnel) |
| Rule 3 | ANY | ANY | ANY | ANY | DISCARD |

The ESP tunnel's outer source address is PAC-TOA and outer destination address is EP-ADDR.

EP's SPD:

| Rule | LADDR | RADDR | LPORT | RPORT | Action |
|---|---|---|---|---|---|
| Rule 1 | PAA-ADDR | ANY | PANA_PORT | ANY | BYPASS |
| Rule 2 | ANY | PAC-TIA | ANY | ANY | PROTECT (ESP, tunnel) |
| Rule 3 | ANY | ANY | ANY | ANY | DISCARD |

The ESP tunnel's outer source address is EP-ADDR and outer destination address is PAC-TOA.

The phase 2 identities (a.k.a. traffic selectors in IKEv2) differ depending on how the PaC acquires the PAC-TIA.

- If the client uses PAC-TOA as the PAC-TIA, then it uses PAC-TOA as the client identity (IDci). The responder identity (IDcr) would contain the ID_IPV4_ADDR_RANGE with starting address as zero address (0.0.0.0) and end address as (255.255.255.255).

- If the client uses [RFC3456] for acquiring the PAC-TIA, it needs to establish the DHCP SA first. This requires additional SPD entries. Once the PAC-TIA is acquired using DHCP, the DHCP SA is deleted and a new IPsec tunnel mode SA is established as specified in this document. When establishing such an SA, PAC-TIA will be used as the IDci. The responder identity (IDcr)would contain the ID_IPV4_ADDR_RANGE with starting address as zero address (0.0.0.0) and end address as (255.255.255.255).

- If IKEv2 is used to obtain the PAC-TIA, the client uses the configuration request (CFG_REQUEST) along with the traffic selectors as given in IKEv2. PaC uses IPV4_ADDR_RANGE with starting address as zero address (0.0.0.0) and end address as (255.255.255.255) for both TSi and TSr. The EP assigns the address (PAC-TIA) and returns it in both the configuration payload (CFG_REPLY) and TSi. The TSr is left to contain the IPV4_ADDR_RANGE.

## 8.2 IPv6 SPD entries

Pac's SPD:

| Rule | LADDR | RADDR | LPORT | RPORT | ITYPE | Action |
|---|---|---|---|---|---|---|
| Rule 1 | ANY | ANY | ANY | ANY | 130-137 | BYPASS |
| Rule 2 | ANY | ANY | PANA_PORT | ANY | ANY | BYPASS |
| Rule 3 | PAC-TIA | ANY | ANY | ANY | ANY | PROTECT (ESP, tunnel) |
| Rule 4 | ANY | ANY | ANY | ANY | ANY | DISCARD |

The ESP tunnel's outer source address is PAC-TOA and outer destination address is EP-ADDR.

EP's SPD:

| Rule | LADDR | RADDR | LPORT | RPORT | ITYPE | Action |
|---|---|---|---|---|---|---|
| Rule 1 | ANY | ANY | ANY | ANY | 130-137 | BYPASS |
| Rule 2 | ANY | ANY | ANY | PANA_PORT | ANY | BYPASS |
| Rule 3 | ANY | PAC-TIA | ANY | ANY | ANY | PROTECT (ESP, tunnel) |
| Rule 4 | ANY | ANY | ANY | ANY | ANY | DISCARD |

The ESP tunnel's outer source address is EP-ADDR and outer destination address is PAC-TOA.

IKEv2 [IKEV2] is used to configure the PAC-TIA address. The usage of traffic selectors is very similar to the IPv4 usage as explained in

the previous section. The client may use the interface identifier in the lower bits of the TSi so that the responder can assign an IPv6 address honoring the interface identifier also.

## 9.0 Dual Stack Operation

IKEv2 [IKEV2] can enable configuration of IPsec-TIA for both IPv4 and IPv6 TIAs by sending both IPv4 and IPv6 configuration attributes in the configuration request (CFG_REQUEST). This enables use of single IPsec tunnel mode SA for sending both IPv4 and IPv6 traffic.





Therefore, IKEv2 is recommended for handling dual-stack PaCs where single execution of IKE is desired.

## 10.0 IANA Considerations

This document does not make no request to IANA.

## 10.0 Security considerations

This document discusses the use of IPsec for access control when PANA is used for authenticating the clients to the access network.

The aggressive mode in IKE [RFC2409] is considered bad due to its DoS properties i.e., any attacker can bombard IKE aggressive mode packets making the EP perform heavy diffie-hellman calculations. As the ID_KEY_ID can be verified by the EP before doing the diffie-hellman calculation, it prevents random attacks. The attacker now needs to listen on the traffic between PaC and PAA to originate IKE requests with valid ID_KEY_ID.

If the EP does not verify whether the PaC is authorized to use an IP address, it is possible for the PaC to steal the traffic destined to some other PaC. When IKEv2 [IKEV2] and [RFC3456] are used for address configuration, the address is assigned by the EP and hence this attack is not present in such cases. When the same address is used as both IPsec-TIA and IPsec-TOA, the EP creates the SPD entry with the appropriate address for the PaC and hence the address is verified implicitly by the virtue of successful IPsec SA negotiation.

## 11.0 Normative References

Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.

[RFC2401] S. Kent et al., "Security Architecture for the Internet Protocol", RFC 2401, November 1998

[PANA-PROT] D. Fosberg et al., "Protocol for Carrying Authentication for Network Access", draft-ietf-pana-06.txt

[RFC4016] M. Parthasarathy, "Protocol for carrying Authentication for Network Access (PANA) Threat analysis and security requirements", RFC 4016, March 2005

12.0 Informative References





[PANAREQ] A. Yegin et al., "Protocol for Carrying Authentication for Network Access (PANA) Requirements and Terminology", draft-ietf-pana-requirements-09.txt

[PANA-FRAME] P. Jayaraman et al., "PANA Framework", draft-ietf-pana-framework-01.txt

[RFC2119] S. Bradner, "Key words for use in RFCS to indicate requirement levels", RFC 2119, March 1997

[RFC2409] D. Harkins et al., "Internet Key Exchange", RFC 2409, November 1998

[IKEV2] C. Kauffman et al., "Internet Key Exchange(IKEv2) Protocol", draft-ietf-ipsec-ikev2-15.txt

[IPSEC-BIS] S. Kent, "Security Architecture for the Internet Protocol", draft-ietf-ipsec-rfc2401bis-06.txt

[RFC2131] R. Droms, "Dynamic Host Configuration Protocol", RFC 2131, March 1997

[RFC3456] B. Patel et al., "Dynamic Host Configuration Protocol (DHCPv4) Configuration of IPsec Tunnel Mode", RFC 3456, January 2003

[RFC3315] R. Droms et. al, "Dynamic Host Configuration Protocol for IPv6", RFC 3315, July 2003

[RFC2461] T. Narten et al., "Neighbor Discovery for IP version 6 (IPv6) ", RFC 2461, December 1998

[RFC2462] S. Thomson et. al, "IPv6 Stateless Address Autoconfiguration", RFC 2462, December 1998

[RFC3041] T. Narten et al., "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 3041, January 2001

[EAP-KEY] B. Aboba et al., "EAP Key Management Framework", draft-ietf-eap-keying-06.txt

[RFC3971] J. Arkko et al., "SEcure Neighbor Discovery (SEND)", RFC 3971, March 2005

[IPV4-LINK] B. Aboba et al., "Dynamic configuration of Link-local IPv4 addresses", draft-ietf-zeroconf-ipv4-linklocal-12.txt

[RFC1918] Y. Rekhter et al., "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996





[RFC2710] S.Deering et al., "Multicast Listener Discovery (MLD)for IPv6", RFC 2710, October 1999

[IEEE80211i] IEEE Draft 802.11I/D5.0, "Draft Supplement to STANDARD FOR Telecommunications and Information Exchange between Systems LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer specifications: Specification for Enhanced Security", August 2003.

## 13.0 Acknowledgments

The author would like to thank Francis Dupont, Pasi Eronen, Yoshihiro Ohba, Jari Arkko, Hannes Tschofenig, Alper Yegin, Erik Nordmark, Giaretta Gerardo, Rafa Marin Lopez, Tero Kivinen and other PANA WG members for their valuable comments and discussions.

## 14.0 Revision log

Changes between revision 06 and 07

-Changed the format of the SPD to use a table
-Changed the IPv6 SPD entries to use ICMPv6 types

Changes between revision 05 and 06

-Clarified that PRPA can be a global address also in IPv6.

Changes between revision 04 and 05

-working group last call comments (mostly editorial)

Changes between revision 03 and 04

-Comments from Erik Nordmark (mostly editorial)

Changes between revision 02 and 03

-Clarified the use of key-Id in ID_KEY_ID payload
-Clarified the address configuration issues.
-Added an Appendix to clarify implementation issues.

Changes between revision 01 and 02

-Updated the draft with the fixes for all open issues
-Added the IP configuration section
-Modified the IKE pre-shared key derivation to handle PAA controlling multiple EPs
-Clarification regarding DHCP usage and RFC3456 usage.





-Only aggressive mode to be supported. Main mode not needed anymore.

Changes between revision 00 and 01

-Specified the use of ESP tunnel mode SA instead of IP-IP transport mode SA after working group discussion.
-Specified the IKE pre-shared key derivation.

## 15.0 Appendix A

This section describes the alternate address configuration methods for Post-PANA address (POPA) and the issues associated with it. As mentioned in section 4, there are multiple ways by which the PaC may configure the POPA address. Only [IKEV2] and [RFC3456] address

configuration methods were described in section 4. Other possibilities and the issues are as follows.

1) Some IKEv1 implementations support IKEv1 MODECFG for configuring IP address. There is no RFC describing MODECFG feature of IKEv1. Also, there is not much information on its widespread support among the implementations. Hence, this document does not recommend it.

2) The address may also be obtained using DHCP [RFC2131] [RFC3315] before the IKE exchange starts. Normally the implementations associate the address and other configuration information (e.g., the default router address) with the interface on which the DHCP is performed. This can cause problems with implementations if they attempt to use an IP address that is configured via [RFC2131] [RFC3315] on the physical interface and use it as the IPsec-TIA on the IPsec tunnel interface. This may work without problems when the IPsec-TIA and IPsec-TOA are same as the IPv4 PRPA that was obtained using DHCP, as the source address selection has to deal with just one address. But using an IPv4 IPsec-TOA different than the IPsec-TIA on a single interface may cause source address selection problem, as there is more than one address to be dealt with. Similarly, an IPv6 address obtained and maintained through a physical link but used on a tunnel interface requires additional implementation considerations. Therefore, this document does not handle the case where DHCP is used to acquire an address for the IPsec-TIA that is different from the IPsec-TOA. Note that this case is different from the address configuration using [RFC3456], which also uses DHCP. When [RFC3456] is used, DHCP is run over the IPsec tunnel and the address (IPsec-TIA) is typically assigned to the IPsec tunnel interface. The IPsec-TOA is assigned to the physical interface. As there is only one address on each interface, there are no address selection issues.





3) The address may also be obtained using auto-configuration [RFC2461] including the temporary addresses described in [RFC3041]. The problem described above for DHCP applies to this also. The implementations would associate the auto-configured addresses and the default router with the interface on which the router advertisement was received. As we configure the SPD to bypass IPsec for router discovery and neighbor discovery messages, the address would be associated with the physical

interface and not with the IPsec interface. There is also an additional issue, as the address configured by the PaC is not known to the EP. It needs to trust whatever PaC provides in its traffic selector during the IPsec SA negotiation. This leads to a DoS attack where the PaC can steal some other PaC's address, which cannot be prevented unless [RFC3971] is deployed.

## 16.0 Author's Addresses

Mohan Parthasarathy
313 Fairchild Drive
Mountain View CA-94043

Email: mohanp@sbcglobal.net

## Intellectual Property Statement

## Disclaimer of Validity



## Copyright Statement



## Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.