IPv6 Operations WG
Internet-Draft
Expires: June 16, 2005

R. Graveman
RFG Security, LLC
M. Parthasarathy
Nokia
P. Savola
CSC/FUNET
H. Tschofenig
Siemens
December 16, 2004

Using IPsec to Secure IPv6-over-IPv4 Tunnels
draft-tschofenig-v6ops-secure-tunnels-03.txt

Abstract

This document gives guidance on securing IPv6-in-IPv4 tunnels using IPsec. No additional protocol extensions are described beyond those

available with the IPsec framework. This document describes packet formats, IPsec security policy database for various scenarios, address configuration procedures, and the usage of the Extensible Authentication Procotol.

Table of Contents

1. Introduction

The IPv6 operations (v6ops) working group has selected IPv6-in-IPv4 tunneling [I-D.ietf-v6ops-mech-v2] as one of the IPv6 transition mechanisms for IPv6 deployment. A number of threats have been identified with possible solutions to mitigate them [I-D.ietf-v6ops-mech-v2]. One of the solutions is the use of IPsec protected tunnels, but there is little detail on how IPsec would actually be used in an interoperable manner. This memo describes the use of IPsec in detail.

First this document analyses the threats that can be addressed by IPsec. Next, this document discusses some of the assumptions made by this document for successful IPsec SA establishment. Then, it gives the details of IKE/IPsec exchange with packet formats and SPD entries. Finally, it discusses the usage of IPsec NAT-traversal mechanism that can be used with configured tunnels in some scenarios.

2. Threats and the Use of IPsec

Following threats have been identified in [I-D.ietf-v6ops-mech-v2]:

1. IPv4 address of the encapsulating ("outer") packet can be spoofed.

2. IPv6 address of the encapsulated ("inner") packet can be spoofed.

The reason for threat (1) is due to the lack of widespread deployment of IPv4 ingress filtering. The reason for threat (2) is that the IPv6 packet is encapsulated in IPv4 and hence escapes IPv6 ingress filtering. [I-D.ietf-v6ops-mech-v2] specifies following strict address checks as mitigating measures.

To mitigate threat (1), the decapsulator verifies that the IPv4 source address of the packet is the same as the address of the configured tunnel endpoint. The decapsulator may also implement IPv4 ingress filtering, i.e., checks whether the packet is received on a legitimate interface.

To mitigate threat (2), the decapsulator verifies whether the inner IPv6 address is a valid IPv6 address and also applies IPv6 ingress filtering before accepting the IPv6 packet.

This memo proposes using IPsec for providing stronger security in preventing these threats. IPsec can be used in two ways, in transport and tunnel mode.

2.1 IPsec in Transport Mode

In transport mode, the IPsec security association (SA) is established to protect the traffic defined by (IPv4-source, IPv4-dest, protocol = 41). On receiving such an IPsec packet, the receiver first applies the IPsec transform (ESP) and then matches the packet against the inbound selectors associated with the SA to verify that the packet is appropriate for the SA via which it was received. The successful verification implies that the packet came from the right IPv4 endpoint as the SA is bound to the IPv4 source address.

This prevents threat (1) but not the threat (2). IPsec in transport mode does not verify the contents of the payload itself where the IPv6 addresses are carried, that is, two nodes that are using IPsec transport mode to secure the tunnel can spoof the inner payload. The packet will be decapsulated successfully and accepted.

The shortcoming can be mitigated by IPv6 ingress filtering i.e., check that the packet is arriving from the interface in the direction of the route towards the tunnel end-point, similar to a Strict Reverse Path Forwarding (RPF) check [RFC3704].

For performing ingress filtering, it is assumed that the tunnel is modelled as an interface and the traffic of the tunnel is protected using IPsec transport mode SA.

2.2 IPsec in Tunnel Mode

In tunnel mode, the IPsec SA is established to protect the traffic defined by (IPv6-source, IPv6-destination). On receiving such an IPsec packet, the receiver first applies the IPsec transform (ESP) and then matches the packet against the inbound selectors associated with the SA to verify that the packet is appropriate for the SA via which it was received. The successful verification implies that the packet came from the right IPv6 endpoint as the SA is bound to the IPv6 source address.

The IPv4 addresses may be spoofed and IPsec cannot detect it in this mode, that is, two nodes that are using IPsec tunnel mode to secure the tunnel with a common tunnel endpoint can spoof each other's IPv4 address. But, the packet will not be accepted by IPsec as the IPv6 address bound to the SA will not match the address in the spoofed packet. Thus, the outer address spoofing is irrelevant as long as the inner IPv6 packet can be verified to come from the right IPv6 endpoint.

3. Scenarios and Overview

There are roughly three kinds of scenarios: (generic) router-to-router tunnels, site-to-router/router-to-site tunnels (a generalization of host-to-router/router-to-host scenarios, respectively), and host-to-host tunnels.

3.1 Router-to-Router Tunnels

IPv6/IPv4 hosts and routers can tunnel IPv6 datagrams over regions of IPv4 routing topology by encapsulating them within IPv4 packets. Tunneling can be used in a variety of ways.

```
.--------.          _----_          .--------.
|v6-in-v4|        _( IPv4 )_        |v6-in-v4|
| Router | <======( Internet )=====> | Router |
|   A    |        (_      _)        |   B    |
'--------'          '----'          '--------'
    ^        IPsec tunnel between        ^
    |        Router A and Router B       |
    V                                    V
```

Figure 1: Router-to-Router Scenario

IPv6/IPv4 routers interconnected by an IPv4 infrastructure can tunnel IPv6 packets between themselves. In this case, the tunnel spans one segment of the end-to-end path that the IPv6 packet takes.

The source and destination addresses of the IPv6 packets traversing the tunnel could come from a wide range of IPv6 prefixes. It is not scalable to establish IPsec tunnel mode SAs for all such packets. Hence, IPsec transport mode SA is recommended for this scenario. IPv6 ingress filtering should be performed to mitigate the IPv6 address spoofing threat.

A specific case of router-to-router tunnels, when one router resides at an end site, is described in the next section.

3.2 Site-to-Router/Router-to-Site Tunnels

This is a generalization of host-to-router and router-to-host tunneling, because the issues when connecting a whole site (using a router), and connecting a single host are roughly equal.

```
      _----_        .---------. IPsec     _----_    IPsec  .-------.
    _( IPv6 )_      |v6-in-v4 | Tunnel  _( IPv4 )_  Tunnel | V4/V6  |
   ( Internet )<--->| Router  |<=======( Internet )=======>| Site B |
    (_      _)      |   A     |        (_      _)          '--------'
      '----'        '---------'          '----'
        ^
        |
        V
    .--------.
    | Native |
    | IPv6   |
    | node   |
    '--------'
```

Figure 2: Router-to-Site Scenario

IPv6/IPv4 routers can tunnel IPv6 packets to their final destination IPv6/IPv4 site. This tunnel spans only the last segment of the end-to-end path.

This is the same as the Site-to-Router case.

```
                                +---------------------+
                                |      IPv6 Network   |
                                |                     |
   .--------.       _----_      |     .--------.      |
   | V6/V4  |     _( IPv4 )_    |     |v6-in-v4|      |
   | Site B |<====( Internet )==========>| Router |      |
   '--------'      (_      _)   |     |   A    |      |
                     '----'     |     '--------'      |
           IPsec tunnel between |         ^           |
           V6 Site and Router A |         |           |
                                |         V           |
                                |     .-------.       |
                                |     |  V6    |      |
                                |     |  Host  |      |
                                |     '--------'      |
                                +---------------------+
```

Figure 3: Site-to-Router Scenario

IPv6/IPv4 hosts can tunnel IPv6 packets to an intermediary IPv6/IPv4 router that is reachable via an IPv4 infrastructure. This type of tunnel spans the first segment of the packet's end-to-end path.

Here, the hosts in the site originate the packets with source addresses coming from a well known prefix whereas the destination address could be any node on the Internet.

In this case, the IPsec tunnel mode SA can be bound to the prefix that was allocated to the router at Site B and router A can verify that the source address of the packet matches the prefix. Site B will not be able to do a similar verification for the packets it receives. This may be quite reasonable for most of the deployment cases, for example, the ISP allocating a /48 to a customer. The CPE (where the tunnel is terminated) "trusts" (in a weak sense) the ISP's router and the ISP's router can verify that the Site B is the only one that can originate packets within the /48.

IPsec tunnel mode SA is recommended for this case which prevents spoofing completely, though similar amount of protection can be obtained with transport mode SA with strict ingress filtering (except for link-local addresses) as well.

3.3 Host-to-Host Tunnels

```
 .--------.           _----_          .--------.
 | V6/V4  |         _( IPv4 )_        | V6/V4  |
 | Host   | <======( Internet )=====> | Host   |
 |   A    |         (_      _)        |   B    |
 '--------'           '----'          '--------'
               IPsec tunnel between
               Host A and Host B
```

Figure 4: Host-to-Host Scenario

IPv6/IPv4 hosts that are interconnected by an IPv4 infrastructure can tunnel IPv6 packets between themselves. In this case, the tunnel spans the entire end-to-end path that the packet takes.

In this case, the source and the destination IPv6 address are known a priori. A tunnel mode SA can be bound to the specific address. The address verification prevents IPv6 address spoofing completely.

4. IKE and IPsec Versions

This section discusses the different versions of the IKE and IPsec security architecture and its applicability to this document.

IPsec security architecture is defined in [RFC2401] and [I-D.ietf-ipsec-rfc2401bis]. There are several differences between them. The difference relevants to this document are discussed below.

1. [RFC2401] does not allow IP as the next layer protocol in traffic selectors when IPsec SA is negotiated. [I-D.ietf-ipsec-rfc2401bis] allows IP also as the next layer protocol like TCP or UDP in traffic selectors.

2. [RFC2401] does not support transport mode SAs between hosts and security gateways. [I-D.ietf-ipsec-rfc2401bis] supports transport mode SA between hosts and security gateway to provide link security e.g., IP-IP tunnel protected with IPsec.

3. [I-D.ietf-ipsec-rfc2401bis] assumes IKEv2, as some of the new features cannot be negotiated using IKEv1. It is valid to negotiate multiple traffic selectors for a given IPsec SA in [I-D.ietf-ipsec-rfc2401bis]. This is possible only with [I-D.ietf-ipsec-ikev2]. If [RFC2409] is used, then multiple SAs need to be setup for each of the traffic selector.

Note that the existing implementations based on [RFC2409] may already be able to support the [I-D.ietf-ipsec-rfc2401bis] features described in (1) and (2). If appropriate, the deployment may choose to use them.

IKE is defined in [RFC2409] (which is referred to as IKE in this document) and in [I-D.ietf-ipsec-ikev2] (which is referred to as IKEv2 in this document). IKEv2 supports features that are useful for configuring and securing tunnels which are not present with IKEv1.

1. IKEv2 supports legacy authentication methods by carrying them in EAP payloads. This can be used to authenticate the hosts/sites to the ISP using EAP methods that supports username and password.

2. IKEv2 supports dynamic address configuration which may be used to configure the IPv6 address of the host.

NAT traversal works with both the old and revised IPsec architectures, but the negotiation is integrated with IKEv2.

We do not consider the usage of the IP Authentication Header (AH) [I-D.ietf-ipsec-rfc2402bis] as ESP [I-D.ietf-ipsec-esp-v3] provides security services (such as integrity protection without confidentiality protection using 'NULL' encryption) which are comparable with AH. This is explicitly stated in [I-D.ietf-ipsec-rfc2401bis].

5. IPsec Configuration Details

This section describes details about the IPsec tunnel establishment for protection of IPv4/IPv6 data traffic.

5.1 IPsec Transport mode

This is typically used in Router-to-Router scenario.

The following SPD entries assume that there are two routers Router1 and Router2, whose tunnel endpoint's IPv4 address is denoted by IPV4-TEP1 and IPV4-TEP2 respectively. The implementations that are strictly conformant to [RFC2401] may not be able to setup the IPsec transport mode SA.

Router1's SPD OUT :

```
IF SRC = IPV4-TEP1 && DST = IPV4-TEP2 && protocol = 41
    THEN USE ESP TRANSPORT MODE SA
```

Router1's SPD IN:

```
IF SRC = IPV4-TEP2 && DST = IPV4-TEP1 && protocol = 41
    THEN USE ESP TRANSPORT MODE SA
```

Router2's SPD OUT:

```
IF SRC = IPV4-TEP2 && DST = IPV4-TEP1 && protocol = 41
    THEN USE ESP TRANSPORT MODE SA
```

Router2's SPD IN:

```
IF SRC = IPV4-TEP1 && DST = IPV4-TEP2 && protocol = 41
    THEN USE ESP TRANSPORT MODE SA
```

The IDci and IDcr payloads of IKEv1 carry the IPv4-TEP1, IPV4-TEP2 and protocol value 41 as phase 2 identities. With IKEv2, the traffic selectors are used to carry the same information.

5.2 IPsec Tunnel mode

5.2.1 SPD for Host-to-Host Scenario

The following SPD entries assume that there are two hosts Host1 and Host2, whose IPv6 addresses are denoted by IPV6-EP1 and IPV6-EP2 (global addresses) and IPV4 addresses of the tunnel endpoints are denoted by IPV4-TEP1 and IPV4-TEP2 respectively. The first three entries of the following SPD are used for protecting link-local traffic: specifically Neighbor Discovery [RFC2461] (ND) and Multicast Listener Discovery messages (MLD) [RFC2710].

IKEv2 [I-D.ietf-ipsec-ikev2] provides the ability to negotiate a single SA for multiple traffic selectors. It could be used here to negotiate a single SA for global and link-local entries shown below.

```
   Host1's SPD OUT :

   IF SRC = ::/128 & destination = any
       THEN USE ESP TUNNEL MODE SA:
           outer source = IPv4-TEP1
           outer dest   = IPV4-TEP2

   IF SRC = fe80::/10 & destination = any
       THEN USE ESP TUNNEL MODE SA:
           outer source = IPv4-TEP1
           outer dest   = IPV4-TEP2

   IF SRC = any & destination = fe80::/10
       THEN USE ESP TUNNEL MODE SA:
           outer source = IPv4-TEP1
           outer dest   = IPV4-TEP2

   IF SRC = IPV6-EP1 && DST = IPV6-EP2
       THEN USE ESP TUNNEL MODE SA:
           outer source = IPv4-TEP1
           outer dest   = IPV4-TEP2

   Host1's SPD IN:
   IF SRC = ::/128 & destination = any
       THEN USE ESP TUNNEL MODE SA:
           outer source = IPv4-TEP2
           outer dest   = IPV4-TEP1

   IF SRC = fe80::/10 & destination = any
       THEN USE ESP TUNNEL MODE SA:
           outer source = IPv4-TEP2
           outer dest   = IPV4-TEP1

   IF SRC = any & destination = fe80::/10
       THEN USE ESP TUNNEL MODE SA:
           outer source = IPv4-TEP2
           outer dest   = IPV4-TEP1

   IF SRC = IPV6-EP2 && DST = IPV6-EP1
       THEN USE ESP TUNNEL MODE SA
           outer source = IPV4-TEP2
           outer dest = IPV4-TEP1

   Host2's SPD OUT:

   IF SRC = ::/128 & destination = any
       THEN USE ESP TUNNEL MODE SA:
           outer source = IPv4-TEP2
```

```
          outer dest   = IPV4-TEP1

   IF SRC = fe80::/10 & destination = any
       THEN USE ESP TUNNEL MODE SA:
           outer source = IPv4-TEP2
           outer dest   = IPV4-TEP1

   IF SRC = any & destination = fe80::/10
       THEN USE ESP TUNNEL MODE SA:
           outer source = IPv4-TEP2
           outer dest   = IPV4-TEP1

   IF SRC = IPV6-EP2 && DST = IPV6-EP1
       THEN USE ESP TUNNEL MODE SA
           outer source = IPv4-TEP2
             outer dest = IPV4-TEP1

   Host2's SPD IN:

   IF SRC = ::/128 & destination = any
       THEN USE ESP TUNNEL MODE SA:
           outer source = IPv4-TEP1
           outer dest   = IPV4-TEP2

   IF SRC = fe80::/10 & destination = any
       THEN USE ESP TUNNEL MODE SA:
           outer source = IPv4-TEP1
           outer dest   = IPV4-TEP2

   IF SRC = any & destination = fe80::/10
       THEN USE ESP TUNNEL MODE SA:
           outer source = IPv4-TEP1
           outer dest   = IPV4-TEP2

   IF SRC = IPV6-EP1 && DST = IPV6-EP2
       THEN USE ESP TUNNEL MODE SA:
           outer source = IPv4-TEP1
          outer dest = IPV4-TEP2
```

The IDci and IDcr payloads of IKEv1 carry the IPV6-EP1 and IPV6-TEP2 or the link-local addresses from the packet headers as phase 2 identities. With IKEv2, the traffic selectors are used to carry the same information.

5.2.2 SPD for Host-to-Router scenario

The following SPD entries assume that the host has the IPv6 address IPV6-EP1 and the tunnel end points of the host and router are

IPV4-TEP1 and IPV4-TEP2 respectively. If the tunnel is between a router and a host where the router has allocated a IPV6-PREF/48 to the host, the corresponding SPD entries can be derived by substituting IPV6-EP1 by IPV6-PREF/48. The first three entries of the following SPD are used for protecting link-local traffic: specifically Neighbor Discovery (ND) and Multicast Listener Discovery messages (MLD).

IKEv2 [I-D.ietf-ipsec-ikev2] provides the ability to negotiate a single SA for multiple traffic selectors. It could be used here to negotiate a single SA for global and link-local entries shown below.

Host's SPD OUT:

```
IF SRC = ::/128 & destination = any
    THEN USE ESP TUNNEL MODE SA:
        outer source = IPv4-TEP1
        outer dest   = IPV4-TEP2

IF SRC = fe80::/10 & destination = any
    THEN USE ESP TUNNEL MODE SA:
        outer source = IPv4-TEP1
        outer dest   = IPV4-TEP2

IF SRC = any & destination = fe80::/10
    THEN USE ESP TUNNEL MODE SA:
        outer source = IPv4-TEP1
        outer dest   = IPV4-TEP2

IF SRC = IPV6-EP1 && DST = any
    THEN use ESP TUNNEL MODE SA
        outer source = IPV4-TEP1
        outer dest   = IPV4-TEP2
```

Host's SPD IN:

```
IF SRC = ::/128 & destination = any
    THEN USE ESP TUNNEL MODE SA:
        outer source = IPv4-TEP2
        outer dest   = IPV4-TEP1

IF SRC = fe80::/10 & destination = any
    THEN USE ESP TUNNEL MODE SA:
        outer source = IPv4-TEP2
        outer dest   = IPV4-TEP1

IF SRC = any & destination = fe80::/10
```

```
        THEN USE ESP TUNNEL MODE SA:
            outer source = IPv4-TEP2
            outer dest   = IPV4-TEP1

    IF SRC = any && DST = IPV6-EP1
        THEN use ESP TUNNEL MODE SA
            outer source = IPV4-TEP2
            outer dest   = IPV4-TEP1

    Router's SPD OUT:

    IF SRC = ::/128 & destination = any
        THEN USE ESP TUNNEL MODE SA:
            outer source = IPv4-TEP2
            outer dest   = IPV4-TEP1

    IF SRC = fe80::/10 & destination = any
        THEN USE ESP TUNNEL MODE SA:
            outer source = IPv4-TEP2
            outer dest   = IPV4-TEP1

    IF SRC = any & destination = fe80::/10
        THEN USE ESP TUNNEL MODE SA:
            outer source = IPv4-TEP2
            outer dest   = IPV4-TEP1

    IF SRC = any && DST = IPV6-EP1
        THEN use ESP TUNNEL MODE SA
            outer source = IPV4-TEP2
            outer dest   = IPV4-TEP1

    Router's SPD IN:

    IF SRC = ::/128 & destination = any
        THEN USE ESP TUNNEL MODE SA:
            outer source = IPv4-TEP1
            outer dest   = IPV4-TEP2

    IF SRC = fe80::/10 & destination = any
        THEN USE ESP TUNNEL MODE SA:
            outer source = IPv4-TEP1
            outer dest   = IPV4-TEP2

    IF SRC = any & destination = fe80::/10
        THEN USE ESP TUNNEL MODE SA:
            outer source = IPv4-TEP1
            outer dest   = IPV4-TEP2
```

```
IF SRC = IPV6-EP1 && DST = any
    THEN use ESP TUNNEL MODE SA
        outer source = IPV4-TEP1
        outer dest   = IPV4-TEP2
```

The IDci and IDcr payloads of IKEv1 carry the IPV6-EP1 and ID_IPV6_ADDR_RANGE or ID_IPV6_ADDR_SUBNET as its phase 2 identity. The starting address is zero IP address and the end address is all ones for ID_IPV6_ADDR_RANGE. The starting address is zero IP address and the end address is all zeroes for ID_IPV6_ADDR_SUBNET. Link-local addresses from the packet would be used if the packet matches the first three selector entries of the SPD. With IKEv2, the traffic selectors are used to carry the same information.

The packet format is the same for both transport mode and tunnel mode as shown in Figure 8.

```
IPv4 header      (source = IPV4-TEP1,
                  destination = IPV4-TEP2)
ESP  header
IPv6 header      (source = IPV6-EP1,
                  destination = IPV6-EP2)
```

Figure 8: Packet Format for transport and tunnel mode

6. Dynamic Address Configuration

With the exchange of protected configuration payloads, IKEv2 is able to provide the IKEv2 peer with DHCP-like information payloads. These configuration payloads are exchanged between the IKEv2 initiator and the responder.

This can be used by the host in the host-to-router scenario to obtain the IPv6 address from the ISP as part of setting up the IPsec tunnel mode SA.

7. Extensible Authentication Support

In addition to the authentication mechanisms provided in IKEv2 the Extensible Authentication Protocol (EAP) [I-D.ietf-eap-rfc2284bis] is included which provides some flexibility for authentication mechanisms. The usage of EAP offers two interesting features:

- o User authentication is terminated at a different entity other than the IKEv2 responder. This allows users' security credentials to be kept in a central place (e.g., AAA server) and to terminate the EAP method at this entity instead at the IKEv2 responder.

Authorization can also be executed at the same entity.

o A number of authentication and key exchange protocols are supported via EAP method (such as EAP-AKA, EAP-SIM, SRP, etc.). Each EAP methods provides its own properties and usage environment. This provides a certain degree of flexibility.

Note that IKEv2 with EAP authentication still requires public key based authentication of the IKEv2 responder outside the EAP authentication. In most deployments this requires a server-side public-key based authentication to protect the EAP exchange with a uni-lateral authenticated tunnel. This method can be used in the host-to-router scenario, where the host can use the traditional (username, password) mechanism to authenticate to the router (ISP) without needing additional configuration for IKE.

8. NAT Traversal

Network address (and port) translation devices are commonly found in today's networks. A detailed description of the problem of IPsec protected data traffic traversing a NAT including requirements are discussed in [RFC3715].

IKEv2 can detect the presence of a NAT automatically by sending an Informational exchange with NAT_DETECTION_SOURCE_IP and NAT_DETECTION_DESTINATION_IP payloads before establishing an IPsec SA. These payloads are processed the same way as in the initial IKE_SA_INIT exchange. Once a NAT is detected and both end points support IPsec NAT traversal extensions UDP encapsulation can be enabled.

More details about UDP encapsulation of IPsec protected IP packets can be found in [I-D.ietf-ipsec-udp-encaps].

For IPv6-over-IPv4 tunneling, NAT traversal is interesting for two reasons:

1. One of the tunnel endpoints is often behind a NAT, and configured tunneling, using protocol 41, is not guaranteed to traverse the NAT. Hence, using IPsec tunnels would enable one to both set-up a secure tunnel, and set-up a tunnel where it might not always be possible without other tunneling mechanisms.

2. Using NAT traversal allows the outer address to change without having to renegotiate the SAs. This could be very beneficial for a crude form of mobility, and in scenarios the NAT changes the IP addresses frequently. However, as the outer address may change, this might introduce new security issues, and using tunnel mode

would be most appropriate.

9. Tunnel Endpoint Discovery

The IKEv2 initiator needs to know the address of the IKEv2 responder to start IKEv2 signaling. A number of ways can be used to provide the initiator with this information, for example:

- o Using off-band mechanisms, e.g., from the ISP's web page.
- o Using DNS to look up a service name by appending it to the DNS search path provided by DHCPv4 (e.g. "tunnel-service.example.com").
- o Using a DHCP option.
- o Using a pre-configured or pre-determined IPv4 anycast address.
- o Using other, unspecified or proprietary methods such as TED (see [I-D.fluhrer-ted]).

For the purpose of this document it is assumed that this address can be obtained somehow. Once the address has been learned, it is configured as the tunnel end-point for the configured IPv6-over-IPv4 tunnel.

This problem is also discussed at more length in [I-D.palet-v6ops-tun-auto-disc].

10. IANA Considerations

This memo makes no request to IANA. [[Please remove this section at publication]]

11. Security Considerations

When you run IPv6-in-IPv4 tunnels (unsecured) over the Internet, it is possible to "inject" packets in the tunnel by spoofing the source address (data plane security), or if the tunnel is signalled somehow (e.g., some messages where you authenticate to the server, so that you would get a static v6 prefix), someone might be able to spoof the signalling (control plane security).

To add security to both, the protocol for tunnel setup and to the data traffic, the IPsec framework plays an important role.

IKE is a signaling protocol with optional Denial of Service protection which authenticates both end points (with different identifities) and establishes two types of security associations (CHILD-SAs and IKE-SA). The authentication mechanisms are very flexible due to the built-in support for symmetric and asymmetric cryptography (or even a combination of both) and the Extensible Authentication Protocol support. The IKE-SA is used to secure most of the IKE message exchange. In particular the CHILD-SA exchange, Informational exchanges (such as the dead-peer detection mechanisms used for liveness checks) and the exchange of configuration messages are secured. The CHILD-SA exchange leads to the establishment of a IPsec tunnel and the creation of SAD and SPD entries.

As a summary, IKE provides a secure signaling protocol for establishing, maintaining and deleting an IPsec tunnel.

IPsec, with the Encapsulating Security Payload (ESP), offers integrity and data origin authentication, confidentiality, with optional (at the discretion of the receiver) anti-replay features. The usage of confidentity-only is discouraged. ESP furthermore provides limited traffic flow confidentality.

IPsec provides access control mechanisms through the distribution of keys and also through the usage of policies dictated by the Security Policy Database (SPD). Furthermore, through the usage of EAP and the backend AAA infrastructure it is possible to enforce additional authorization mechanisms (at the user level) at entities other than the tunnel end points.

The NAT traversal mechanism provided by IKE introduces some weaknesses into IKE and IPsec. These issues are discussed in more detail in [I-D.ietf-ipsec-ikev2].

Please note that the usage of IPsec for the scenarios described in Figure 3, Figure 2 and Figure 1 does not aim to protect the end-to-end communication. It protects just the tunnel part. It is still possible for an IPv6 endpoint that is not attached to the IPsec tunnel to spoof packets.

12. Open Issues

This section lists some open issues for which feedback/text would be especially useful, and will be resolved in one way or another in a future revision.

- o Discussion of 'Use of IPsec Transport Mode for Dynamic Routing' [I-D.touch-ipsec-vpn] might be appropriate.

- o A more detailed description of the address configuration mechanism

would be helpful. The configuration example with CFG_REQUEST/CFG_REPLY payloads should contain IPv6 addresses.

- o Some notes on the implications of mobility interworking are still missing.

- o The "Site-to-Router" scenarios separation is a bit weak -- any better ideas how to categorize these would be appreciated.

- o More extensive discussion of when transport/tunnel mode SAs make sense and would probably be useful.

13. Contributors

The authors are listed in alphabetical order.

Suresh Satapati also participated in the discussions.

14. Acknowledgments

The authors would like to thank Stephen Kent and Michael Richardson for their comments.

We would like to thank Pasi Eronen for his text contributions.

15. References

15.1 Normative References

[I-D.ietf-eap-rfc2284bis]
Blunk, L., "Extensible Authentication Protocol (EAP)", draft-ietf-eap-rfc2284bis-09 (work in progress), February 2004.

[I-D.ietf-ipsec-esp-v3]
Kent, S., "IP Encapsulating Security Payload (ESP)", draft-ietf-ipsec-esp-v3-09 (work in progress), October 2004.

[I-D.ietf-ipsec-ikev2]
Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", draft-ietf-ipsec-ikev2-17 (work in progress), October 2004.

[I-D.ietf-ipsec-rfc2401bis]
Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", draft-ietf-ipsec-rfc2401bis-05 (work

in progress), December 2004.

[I-D.ietf-ipsec-udp-encaps]
Huttunen, A., "UDP Encapsulation of IPsec Packets", draft-ietf-ipsec-udp-encaps-09 (work in progress), May 2004.

[I-D.ietf-v6ops-mech-v2]
Nordmark, E. and R. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers", draft-ietf-v6ops-mech-v2-06 (work in progress), September 2004.

[RFC2461] Narten, T., Nordmark, E. and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998.

[RFC2710] Deering, S., Fenner, W. and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", RFC 2710, October 1999.

15.2 Informative References

[I-D.bellovin-useipsec]
Bellovin, S., "Guidelines for Mandating the Use of IPsec", draft-bellovin-useipsec-03 (work in progress), March 2004.

[I-D.blanchet-v6ops-tunnelbroker-tsp]
Parent, F. and M. Blanchet, "IPv6 Tunnel Broker with the Tunnel Setup Protocol(TSP)", draft-blanchet-v6ops-tunnelbroker-tsp-01 (work in progress), June 2004.

[I-D.fluhrer-ted]
Fluhrer, S., "Tunnel Endpoint Discovery", draft-fluhrer-ted-00 (work in progress), November 2001.

[I-D.ietf-ipsec-rfc2402bis]
Kent, S., "IP Authentication Header", draft-ietf-ipsec-rfc2402bis-10 (work in progress), December 2004.

[I-D.palet-v6ops-tun-auto-disc]
Palet, J. and M. Diaz, "Analysis of IPv6 Tunnel End-point Discovery Mechanisms", draft-palet-v6ops-tun-auto-disc-02 (work in progress), October 2004.

[I-D.touch-ipsec-vpn]
Touch, J., Eggert, L. and Y. Wang, "Use of IPsec Transport

Mode for Dynamic Routing", draft-touch-ipsec-vpn-07 (work in progress), March 2004.

[RFC2401] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[RFC2409] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[RFC3704] Baker, F. and P. Savola, "Ingress Filtering for Multihomed Networks", BCP 84, RFC 3704, March 2004.

[RFC3715] Aboba, B. and W. Dixon, "IPsec-Network Address Translation (NAT) Compatibility Requirements", RFC 3715, March 2004.

Authors' Addresses

Richard Graveman
RFG Security, LLC
15 Park Avenue
Morristown, New Jersey 07960
USA

EMail: rfg@acm.org

Mohan Parthasarathy
Nokia
313 Fairchild Drive
Mountain View CA-94043
USA

EMail: mohanp@sbcglobal.net

Pekka Savola
CSC/FUNET
Espoo
Finnland

EMail: psavola@funet.fi

Hannes Tschofenig
Siemens
Otto-Hahn-Ring 6
Munich, Bayern 81739
Germany

EMail: Hannes.Tschofenig@siemens.com

Acknowledgment

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