RSIP Support for End-to-end IPsec

RFC 3104

Status (/doc/rfc3104/)	IESG evaluation record	IESG writeups (/doc/rfc3104/writeup/)
Email expansions (/doc/rfc3104/email/)	History (/doc/rfc3104/history/)	

Revision differences

From revision

draft-ietf-nat-rsip-ipsec-04 (2000-07-20)	▼

To revision

rfc3104 (2001-10-01)	▼

Diff format

Side-by-side	Before-after	Change bars	Wdiff		Submit

Document history

Date ⬍	Rev. ⬍	By ⬍	Action ⬍
2001-10-01	04	(System)	RFC published
2001-01-25	04	(System)	IESG has approved the document
2000-07-20	04	(System)	New version available: **draft-ietf-nat-rsip-ipsec-04.txt**
2000-03-15	03	(System)	New version available: **draft-ietf-nat-rsip-ipsec-03.txt**
2000-01-31	02	(System)	New version available: **draft-ietf-nat-rsip-ipsec-02.txt**
1999-10-28	01	(System)	New version available: **draft-ietf-nat-rsip-ipsec-01.txt**
1999-05-20	00	(System)	New version available: **draft-ietf-nat-rsip-ipsec-00.txt**

ISOC (https://www.internetsociety.org/)   IETF Trust (https://trustee.ietf.org/)

RFC Editor (https://www.rfc-editor.org/)   IRTF (https://www.irtf.org/)   IESG

(https://www.ietf.org/iesg/)   IETF (https://www.ietf.org/)   IAB (https://www.iab.org/)

IASA & IAOC (https://iaoc.ietf.org)   IETF Tools (https://tools.ietf.org/)   IANA

(https://www.iana.org/)

RSIP Support for End-to-end IPsec
RFC 3104

Status (/doc/rfc3104/) | IESG evaluation record | IESG writeups (/doc/rfc3104/writeup/) | Email expansions (/doc/rfc3104/email/)

History (/doc/rfc3104/history/)

Versions | 04 (/doc/draft-ietf-nat-rsip-ipsec/)

draft-ietf-nat-rsip-ipsec | 00 | 01 | 02 | 03 | 04
rfc3104

May 1999 | Oct 1999 | Jan 2000 | Mar 2000 | Jul 2000
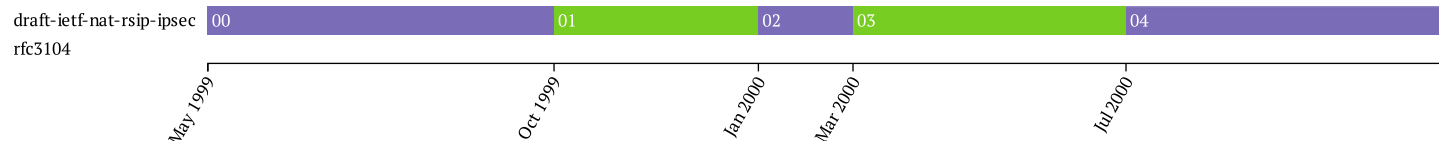
Document	**Type**	RFC - Experimental (October 2001; Errata (https://www.rfc-editor.org/errata_search.php?rfc=3104)) Was draft-ietf-nat-rsip-ipsec (/doc/draft-ietf-nat-rsip-ipsec/) (nat WG (/wg/nat/))
	Last updated	2013-03-02
	Stream	IETF
	Formats	📄 plain text (https://www.rfc-editor.org/rfc/rfc3104.txt) 📄 pdf (https://www.rfc-editor.org/rfc/pdfrfc/rfc3104.txt.pdf) 📄 html (https://tools.ietf.org/html/rfc3104) 📄 bibtex (bibtex)
Stream	**WG state** (/help/state/draft/ietf)	WG Document
	Document shepherd	No shepherd assigned
IESG	**IESG state** (/help/state/draft/iesg)	RFC 3104 (Experimental)
	Consensus Boilerplate	Unknown
	Telechat date	
	Responsible AD	(None)
	Send notices to	(None)

✉ Email authors (mailto:draft-ietf-nat-rsip-ipsec@ietf.org?subject=Mail%20regarding%20draft-ietf-nat-rsip-ipsec)

✉ Email WG (mailto:nat@ietf.org?subject=Mail%20regarding%20draft-ietf-nat-rsip-ipsec) | ⚡ IPR (/ipr/search/?submit=draft&id=draft-ietf-nat-rsip-ipsec)

← References (/doc/rfc3104/references/) | → Referenced by (/doc/rfc3104/referencedby/)

❗ Nits (https://www.ietf.org/tools/idnits?url=https://www.ietf.org/archive/id/draft-ietf-nat-rsip-ipsec-04.txt) | 🔍 Search lists ▾

```
Network Working Group                                      G. Montenegro
Request for Comments: 3104                         Sun Microsystems, Inc.
Category: Experimental                                        M. Borella
                                                              CommWorks
                                                           October 2001


                   RSIP Support for End-to-end IPsec
```

Status of this Memo

```
   This memo defines an Experimental Protocol for the Internet
   community.  It does not specify an Internet standard of any kind.
   Discussion and suggestions for improvement are requested.
   Distribution of this memo is unlimited.
```

Copyright Notice

```
   Copyright (C) The Internet Society (2001).  All Rights Reserved.
```

IESG Note

```
   The IESG notes that the set of documents describing the RSIP
   technology imply significant host and gateway changes for a complete
   implementation.  In addition, the floating of port numbers can cause
   problems for some applications, preventing an RSIP-enabled host from
   interoperating transparently with existing applications in some cases
   (e.g., IPsec).  Finally, there may be significant operational
   complexities associated with using RSIP.  Some of these and other
   complications are outlined in section 6 of the RFC 3102, as well as
   in the Appendices of RFC 3104.  Accordingly, the costs and benefits
   of using RSIP should be carefully weighed against other means of
   relieving address shortage.
```

Abstract

```
   This document proposes mechanisms that enable Realm Specific IP
   (RSIP) to handle end-to-end IPsec (IP Security).
```

```
Montenegro & Borella          Experimental                      [Page 1]
RFC 3104          RSIP Support for End-to-end IPsec         October 2001
```
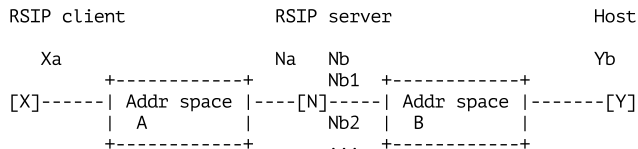
Table of Contents

1. Introduction

```
   This document specifies RSIP extensions to enable end-to-end IPsec.
   It assumes the RSIP framework as presented in [RSIP-FW], and
   specifies extensions to the RSIP protocol defined in [RSIP-P].  Other
   terminology follows [NAT-TERMS].

   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 RFC 2119.
```

2. Model

```
   For clarity, the discussion below assumes this model:

   RSIP client              RSIP server               Host

      Xa                 Na   Nb                       Yb
          +------------+      Nb1  +------------+
   [X]------| Addr space |----[N]-----| Addr space |-------[Y]
          |     A      |      Nb2  |     B      |
          +------------+      ...  +------------+
```

Hosts X and Y belong to different address spaces A and B,
respectively, and N is an RSIP server. N has two addresses: Na on
address space A, and Nb on address space B. For example, A could be
a private address space, and B the public address space of the
general Internet. Additionally, N may have a pool of addresses in
address space B which it can assign to or lend to X.

This document proposes RSIP extensions and mechanisms to enable an
RSIP client X to initiate IKE and IPsec sessions to a legacy IKE and
IPsec node Y. In order to do so, X exchanges RSIP protocol messages
with the RSIP server N. This document does not yet address IKE/IPsec
session initiation from Y to an RSIP client X. For some thoughts on
this matter see Appendix G.

The discussion below assumes that the RSIP server N is examining a
packet sent by Y, destined for X. This implies that "source" refers
to Y and "destination" refers to Y's peer, namely, X's presence at N.

This document assumes the use of the RSAP-IP flavor of RSIP (except
that port number assignments are optional), on top of which SPI
values are used for demultiplexing. Because of this, more than one
RSIP client may share the same global IP address.

3. Implementation Notes

The RSIP server N is not required to have more than one address on
address space B. RSIP allows X (and any other hosts on address space
A) to reuse Nb. Because of this, Y's SPD SHOULD NOT be configured to
support address-based keying. Address-based keying implies that only
one RSIP client may, at any given point in time, use address Nb when
exchanging IPsec packets with Y. Instead, Y's SPD SHOULD be
configured to support session-oriented keying, or user-oriented
keying [Kent98c]. In addition to user-oriented keying, other types
of identifications within the IKE Identification Payload are equally
effective at disambiguating who is the real client behind the single
address Nb [Piper98].

Because it cannot rely on address-based keying, RSIP support for
IPsec is similar to the application of IPsec for remote access using
dynamically assigned addresses. Both cases impose additional
requirements which are not met by minimally compliant IPsec
implementations [Gupta]:

    Note that a minimally-compliant IKE implementation (which only
    implements Main mode with Pre-shared keys for Phase I
    authentication) cannot be used on a remote host with a dynamically
    assigned address. The IKE responder (gateway) needs to look up
    the initiator's (mobile node's) pre-shared key before it can

Montenegro & Borella   Experimental   [Page 3]

RFC 3104   RSIP Support for End-to-end IPsec   October 2001

    decrypt the latter's third main mode message (fifth overall in
    Phase I). Since the initiator's identity is contained in the
    encrypted message, only its IP address is available for lookup and
    must be predictable. Other options, such as Main mode with
    digital signatures/RSA encryption and Aggressive mode, can
    accommodate IKE peers with dynamically assigned addresses.

IKE packets are typically carried on UDP port 500 for both source and
destination, although the use of ephemeral source ports is not
precluded [ISAKMP]. IKE implementations for use with RSIP SHOULD
employ ephemeral ports, and should handle them as follows [IPSEC-
MSG]:

    IKE implementations MUST support UDP port 500 for both source and
    destination, but other port numbers are also allowed. If an
    implementation allows other-than-port-500 for IKE, it sets the
    value of the port numbers as reported in the ID payload to 0
    (meaning "any port"), instead of 500. UDP port numbers (500 or
    not) are handled by the common "swap src/dst port and reply"
    method.

It is important to note that IPsec implementations MUST be aware of
RSIP, at least in some peripheral sense, in order to receive assigned
SPIs and perhaps other parameters from an RSIP client. Therefore,
bump-in-the-stack (BITS) implementations of IPsec are not expected to
work "out of the box" with RSIP.

4. IKE Handling and Demultiplexing

If an RSIP client requires the use of port 500 as its IKE source,
this prevents that field being used for demultiplexing. Instead, the
"Initiator Cookie" field in the IKE header fields must be used for
this purpose. This field is appropriate as it is guaranteed to be
present in every IKE exchange (Phase 1 and Phase 2), and is
guaranteed to be in the clear (even if subsequent IKE payloads are
encrypted). However, it is protected by the Hash payload in IKE

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.

fastcase®
Smarter legal research.