IPSP Working Group   L.A. Sanchez
INTERNET-DRAFT   BBN Technologies
Expire in March, 2001   H. Orman
                                                     Novell Corporation
                                                     November 16, 2000

A Roadmap for IPsec Policy Management
draft-ietf-ipsp-roadmap-01.txt

Status of this Memo

Abstract

   This document describes the approach that the IPSP WG will follow
   to resolve the challenges that IPsec compliant devices phase with
   respect to modeling, specifying, translating, provisioning,
   exchanging, negotiating, checking and enforcing IPsec policies.

1. What is the IPSP WG trying to solve?

   The rapid growth of the Internet and the need to control access to
   network resources (bandwidth, routers, hosts, etc.) has quickly
   generated the need for representing, discovering, exchanging and
   managing the policies that control access to these resources in a
   scalable, secured and reliable fashion.

   Current IP security protocols and algorithms [RFCs 2401-2412, 2085,
   2104 and 2451] can exchange keying material using IKE [RFC2409] and
   protect data flows using the AH [RFC2402] and/or ESP protocols
   [RFC2406]. The scope of IKE limits the protocol to the authenticated
   exchange of keying material and associated policy information between

the end-points of a security association.

However, along the path of a communication, there may be
administrative entities that need to impose policy constraints on
entities such as security gateways and router filters. There also is
a need for end-points of a security association and/or, for their
respective administrative entities, to securely discover and
negotiate access control information for the end hosts and for the
policy enforcement points (security gateways, routers, etc.) along
the path of the communication.

2. Roadmap to a solution

In essence the IPSP WG will produce a set of documents and working
code. To accomplish this the IPSP WG will work on the items listed
below. Please note, that not all items require code
development. Below, you will find a complete list of all
items. The IPSP WG will:

   1) first establish the requirements for IPsec policy
      management. Any solution developed under the IPSP umbrella
      MUST meet these requirements. The requirements document
      will cover all aspects of IPsec policy management including:

            - IPsec data model
            - IPsec policy architecture
            - IPsec policy specification
            - IPsec policy provisioning
            - IPsec security gateway discovery
            - IPsec policy discovery, negotiation, conflict
              resolution and compliance checking

   This WG item will produce a standards-track document.

   2) define a data model for IPsec policies. This model will be
      compatible with the P-CIM [PCIM]. This WG item will
      produce a standards-track document.

   3) develop an architecture for IPsec policy management. The
      document will discuss and cover the following topics:

            - IPsec data model
            - IPsec policy specification
            - IPsec policy provisioning
            - IPsec security gateway discovery
            - IPsec policy discovery, negotiation, conflict
              resolution and compliance checking

   This WG item will produce a standards-track document.

   4) develop a flexible, vendor-independent language to
      represent IPsec policies. The language MUST follow the
      IPsec data model which in turns follows the P-CIM.

   This WG item will produce a standards-track document and
   parser implementations.

   5) develop guidelines for the provisioning of IPsec policies
      using existing policy provisioning protocols. This includes
      profiles for distributing IPsec policies over protocols
      such as LDAP, COPS, SNMPCONF, FTP, etc.

This WG item will produce standards-track documents and
implementations.

6) specify and develop adopt or develop an IPsec policy
   exchange and negotiation protocol. The protocol must be
   capable of:

   i) discovering security gateways
   ii) exchanging and negotiating security policies, and;
   iii) resolving policy conflicts in both intra/inter
        domain environments. The protocol must be
        independent of any security protocol suite and key
        management protocol.

Note that the WG MAY decide to divide the above-mentioned
functionality into one or more protocols. This WG item will
produce a standards-track document and implementations.

3. Roadmap Nutshell

   Requirements document. Standards track.

   Roadmap Document. This is the roadmap document. Standards track.

   Data Information Model. Standards track.

   Policy Management Architecture. Standards track.

   Specification Language. Standards track document and a reference
   implementation of the parser.

   Provisioning Guidelines. Standards track document and implementations
   using existing provisioning protocols.

   Policy Exchange and Negotiation Protocol. At least one standards
   track document and implementation.

4. Security Considerations

   The document provides a framework for applications to identify the
   relevant policies in place across the network. Policies must be
   communicated in a secure way so as not to jeopardize the ability
   of the application to run. It is also important to ensure that the
   policies that are communicated statically or dynamically to the
   Policy Enforcement device are doen so, securely. Not doing so could
   compromise the security of the entire network.

REFERENCES

   [RFC2119] Bradner, S., "Key Words for use in RFCs to indicate
       Requirement Levels", RFC2119, March 1997.

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

   [RFC2403] S. Kent, R. Atkinson, "IP Authentication Header", RFC 2402

   [RFC2406] S. Kent, R. Atkinson, "IP Encapsulating Security Payload
       (ESP)", RFC 2406.

   [PCIM] Moore, et al., "Policy Core Information Model -- Version 1
      Specification"
      ftp://ftp.ietf.org/internet-drafts/draft-ietf-policy-core-info-model-
07.txt

   [RFC2407] D. Piper, "The Internet IP Security Domain of Interpretation
        for ISAKMP", RFC 2407.

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

Authors' Addresses

   Luis A. Sanchez
   BBN Technologies
   GTE Internetworking
   10 Moulton Street
   Cambridge, MA 02140

   Voice: (617) 873-3351
   EMail: lsanchez@bbn.com

   Hilarie Orman
   Novell, Inc.
   Net Content Services
   1800 South Novell Place
   Provo, UT 84606

   Voice: (801)861-5278
   EMail: horman@novell.com