Groupe de travail Réseau
Request for Comments : 3586
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

M. Blaze, AT&T Labs - Research
A. Keromytis, Columbia University
M. Richardson, Sandelman Software Works
L. Sanchez, Xapiens Corporation
août 2003

Exigences de la politique de sécurité IP (IPSP)

Résumé
Le présent document décrit l'espace de problème et les exigences de solution pour développer un cadre de configuration et de gestion d'une politique de sécurité IP (IPSP, *IP Security Policy*). L'architecture IPSP fournit un cadre adaptable décentralisé pour gérer, découvrir et négocier les politiques de sécurité d'hôte et de réseau qui gouvernent l'accès, l'autorisation, l'authentification, la confidentialité, et l'intégrité des données, et les autres propriétés de sécurité IP. Le présent document met en lumière des composants architecturaux et présente leur exigences fonctionnelles.

Table des matières

1. Introduction

1.1 Terminologie

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

1.2 Politique de sécurité et IPsec

La sécurité de la couche réseau jouit actuellement d'une large popularité comme outil pour protéger le trafic Internet et les ressources. La sécurité à la couche réseau peut être utilisée comme outil pour au moins deux sortes d'architecture de sécurité :

a) Passerelles de décurité . les passerelles de sécurité (y compris les "pare-feu") à la bordure des réseaux utilisent IPsec [RFC2401] pour mettre en application le contrôle d'accès, protéger la confidentialité er l'authenticité du trafic entrant et quittant un réseau, et pour fournir des services de passerelle pour les réseaux privés virtuels (VPN, *Virtual Private Network*).

b) Communication sûre de bout en bout : les hôtes utilisent IPsec pour mettre en œuvre le contrôle d'accès au niveau de l'hôte, pour protéger la confidentialité et l'authenticité du trafic réseau échangé avec les hôtes homologues avec lesquels ils communiquent, et pour joindre les réseaux virtuels privés.

D'un côté, IPsec fournit une excellente base pour une très large gamme de schémas de protection ; d'un autre côté, cette large gamme d'applications pour IPsec crée des tâches de gestion complexes qui deviennent particulièrement difficiles avec la croissance des réseaux et exigent des politiques de sécurité différentes, et sont contrôlées par des entités différentes, pour différentes sortes de trafic dans les différentes parties du réseau.

Lorsque les organisations déploient des passerelles de sécurité, l'Internet se divise en régions hétérogènes qui appliquent des politiques d'accès et de sécurité différentes. Il est souvent encore nécessaire aux hôtes de communiquer à travers les frontières de réseau contrôlées par plusieurs politiques différentes. La large gamme des choix de paramètres cryptographiques (aux diverses couches de protocole) complique les choses et introduit le besoin que les hôtes et les passerelles de sécurité identifient et négocient un ensemble de paramètres de sécurité qui satisfassent les exigences de chaque partie. Encore plus de complexité apparaît lorsque IPsec devient le moyen par lequel les pare-feu appliquent le contrôle d'accès et la participation aux VPN ; deux points d'extrémité IPsec qui veulent établir une association de sécurité doivent identifier, non seulement les paramètres cryptographiques mutuellement acceptables, mais aussi exactement quelle sorte d'accès fournissent les politiques de sécurité combinées.

Alors que la négociation des paramètres de chiffrement et autres paramètres de sécurité pour les associations de sécurité (SA, *Security Association*) est prise en charge par les protocoles de gestion de clé (par exemple, ISAKMP [RFC2408]) la couche de gestion de clé IPsec ne fournit pas de schéma pour gérer, négocier, ou appliquer les politiques de sécurité sous lesquelles les SA opèrent.

IPSP fournit le cadre pour gérer la politique de sécurité IPsec, négocier les paramètres des associations de sécurité (SA) entre les points d'extrémité IPsec, et distribuer les informations d'autorisation et de politique parmi les hôtes qui exigent la capacité de communiquer via IPsec.

2. Espace de problème de la politique de sécurité IP

IPSP vise à fournir un cadre adaptable décentralisé pour gérer, découvrir et négocier les politiques Ipsec d'hôte et de réseau qui gouvernent l'accès, l'autorisation, les mécanismes de chiffrement, la confidentialité, l'intégrité des données, et autres propriétés IPsec.

Le problème central résolu par IPSP est celui du contrôle de la politique de sécurité d'une manière utile pour la large gamme des applications et modes de fonctionnement IPsec. En particulier :

- Les hôtes IPSP peuvent servir de points d'extrémité IPsec, de passerelle de sécurité, de plate-forme de gestion de réseaux, ou d'une combinaison de ces fonctions. IPSP va gérer les ordinateurs des utilisateurs d'extrémité (qui peuvent être des stations de travail fixes contrôlées par une seule organisation ou des ordinateurs portables mobiles qui exigent l'accès distant à un VPN d'entreprise) des pare-feu (qui fournissent différents services et permettent différents niveaux d'accès aux différentes classes de trafic et d'utilisateurs) des routeurs de VPN (qui prennent en charge les liaisons aux autres VPN qui peuvent être contrôlés par la politique réseau d'une organisation différente) des serveurs de la Toile et autres (qui peuvent fournir des services différents selon l'endroit d'où provient la demande d'un client) et ainsi de suite.

- L'administration d'IPSP va être par nature hétérogène et décentralisée. Une caractéristique de base de IPsec est que deux hôtes peuvent établir une association de sécurité même si ils ne partagent pas une politique de sécurité commune, ou, bien sûr, ne se font pas du tout confiance. Cette propriété de IPsec devient encore plus prononcée au niveau d'abstraction supérieur géré par IPSP.

- Les paramètres de SA acceptables à toute paire d'hôtes (opérant sous des politiques différentes) vont souvent n'être pas spécifiés à l'avance. IPSP va souvent avoir à négocier et découvrir au vol les paramètres de SA mutuellement acceptables lorsque deux hôtes tentent de créer une nouvelle SA.

- Certains hôtes vont être gouvernés par des politiques qui ne sont pas directement spécifiées dans le langage de IPSP. Par exemple, la politique IPsec d'un hôte pourrait être dérivée d'une politique de sécurité de couche supérieure plus complète gérée par quelque autre système. De même, certains fabricants pourraient développer des outils spécialisés (et brevetés) pour gérer la politique de leurs produits. Dans ce cas, il est nécessaire de déduire une spécification de politique IPSP pour les seuls aspects de la politique d'un hôte qui impliquent l'interopérabilité avec les autres hôtes qui fonctionnent avec IPSP.

- IPSP doit s'adapter à la prise en charge de schémas complexes d'administration de politique. Même dans des réseaux de taille modeste, un administrateur doit souvent contrôler la politique à distance, et doit avoir la capacité de changer la politique sur les nombreux hôtes différents au même moment. Dans les plus grands réseaux (ou ceux qui appartiennent à de grandes organisations) la politique d'un hôte pourrait être gouvernée par plusieurs autorités différentes (par exemple, plusieurs départements différents pourraient avoir l'autorité d'ajouter des utilisateurs à un pare-feu ou ouvrir l'accès à de nouveaux services). Différentes parties d'une politique pourraient être "possédées" par différentes entités dans une hiérarchie complexe. IPSP doit fournir un mécanisme pour déléguer des sortes d'autorités spécifiques à des entités spécifiques.

- La sémantique d'IPSP doit être bien définie, en particulier à l'égard de tout aspect critique pour la sécurité d'un système.

- IPSP doit être sûr, clair, et compréhensible. Il devrait être possible de comprendre ce que fait une politique d'IPSP ; la difficulté de compréhension d'une politique d'IPSP devrait être assez proportionnelle à la complexité du problème à résoudre. Il devrait aussi être possible d'avoir confiance que une politique IPSP fait ce qu'elle prétend faire, et que la mise en œuvre de IPSP est correcte ; architecturalement, les parties critiques pour la sécurité de IPSP devraient être assez petites et bien spécifiées pour permettre la vérification de leur fonctionnement correct. Idéalement, IPSP devrait être compatible avec des méthodes formelles, comme de mettre en œuvre les politiques de sécurité avec des propriétés prouvables.

3. Exigences pour un cadre de configuration et de gestion d'une politique de sécurité IP

3.1 Exigences générales

Une solution d'IPSP DOIT inclure :

- Un modèle de politique avec une sémantique bien définie qui capture les relations entre les SA IPsec et les politiques de sécurité de niveau supérieur,

- Un mécanisme de découverte de passerelles qui permette aux hôtes de découvrir où diriger le trafic IPsec destiné à un point d'extrémité spécifique,

- Un langage bien spécifié pour décrire les politiques des hôtes,

- Un moyen pour répartir les responsabilités des différents aspects de la politique aux différentes entités,

- Un mécanisme pour découvrir la politique d'un hôte,

- Un mécanisme pour résoudre les paramètres spécifiques de IPsec à utiliser entre deux hôtes gouvernés par des politiques différentes (et pour déterminer si de tels paramètres existent) et,

- Un mécanisme bien spécifié pour vérifier la conformité à la politique d'un hôte quand les SA sont créées.

Les mécanismes utilisés dans IPSP ne doivent exiger de modifications de protocole dans aucune des normes IPsec (ESP [RFC2406], AH, [RFC2402], IKE [RFC2409]). Les mécanismes doivent être indépendants du protocole de négociation de SA, mais peuvent supposer certaines fonctionnalités d'un tel protocole (ceci est pour s'assurer que de futurs protocoles de négociation de SA ne sont pas incompatibles avec IPSP).

3.2 Description et justification

3.2.1 Modèle de politique

Un modèle de politique définit la sémantique de la politique IPsec. La spécification, vérification, et résolution de politique devraient mettre en œuvre la sémantique définie dans le modèle. Cependant, le modèle devrait être indépendant du mécanisme spécifique de distribution de politique et du schéma de découverte de politique, dans la mesure du possible.

3.2.2 Découverte de passerelle de sécurité

Le mécanisme de découverte de passerelle peut être invoqué par tout hôte ou passerelle. Son but est de déterminer quelles passerelles IPsec existent entre l'initiateur et l'homologue de communication prévu. Le mécanisme réel employé peut être utilisé pour porter les informations nécessaires à d'autres composants de l'architecture d'IPSP (par exemple, la découverte de politique, comme présenté dans [SPP]). Le mécanisme de découverte peut devoir être invoqué à tout moment, indépendamment des associations de sécurité existantes ou d'autres communications, pour détecter des changements de topologie.

3.2.3 Langage de spécification de politique

Afin de permettre la découverte de politique, la vérification de conformité et la résolution à travers une gamme d'hôtes, un langage commun est nécessaire pour exprimer les politiques des hôtes qui ont besoin de communiquer les uns avec les autres. Les déclarations dans ce langage sont le résultat de la découverte de la politique, et fournissent les entrées des systèmes de résolution de politique et de vérification de conformité. Noter que la politique de sécurité d'un hôte ou d'un réseau peut être exprimée d'une façon spécifique du fabricant, mais serait traduite dans le langage commun lorsque elle doit être gérée par les services IPSP.

3.2.4 Politique répartie

Comme discuté ci-dessus, il doit être possible que tout ou partie de la politique d'un hôte soit gérée à distance, éventuellement par plus d'une entité. C'est une exigence de base pour les réseaux et systèmes à grande échelle.

3.2.5 Découverte de politique

Un mécanisme de découverte de politique doit fournir les informations essentielles que deux points d'extrémité IPsec peuvent utiliser pour déterminer quelles sortes de SA sont possibles entre eux. Ceci est particulièrement important pour les hôtes qui ne sont pas contrôlés par la même entité, et qui pourraient ne pas partager initialement d'informations communes de l'un sur l'autre. Noter qu'un hôte n'a pas besoin de révéler toute sa politique de sécurité, mais seulement assez d'informations pour prendre en charge le système de résolution de SA pour les hôtes qui pourraient vouloir communiquer avec lui.

3.2.6 Résolution d'association de sécurité

Une fois que deux hôtes en ont appris suffisamment sur la politique de l'autre, il doit être possible (et faisable) de trouver un ensemble acceptable de paramètres de SA qui satisfasse les exigences des deux hôtes et conduise à la réussite de la création d'une nouvelle SA.

3.2.7 Vérification de conformité

Quand un hôte propose le résultat d'un schéma de résolution de SA, il doit être vérifié qu'il est conforme à la politique de sécurité locale de chaque hôte. La sécurité et l'adéquation des SA créées par les communications gérées par IPSP devraient ne dépendre que de la correction de l'étape de vérification de conformité. En particulier, même si le schéma de résolution de SA (qui est probablement complexe du point de vue du calcul et de la conception) produit un résultat incorrect, il devrait quand même n'être pas possible de violer la politique spécifiée par l'un ou l'autre des hôtes.

4. Considérations sur la sécurité

Le présent document discute des exigences de haut niveau pour un cadre de politique et d'architecture pour IPsec. Il donne une justification des diverses composantes.

5. Considérations relatives à l'IANA

Aucune action n'est requise de l'IANA.

6. Déclaration de propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourraient être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur le répertoire en ligne des IPR de l'IETF à http://www.ietf.org/ipr .

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf-ipr@ietf.org .

7. Références

7.1 Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

[RFC2401] S. Kent et R. Atkinson, "Architecture de sécurité pour le protocole Internet", novembre 1998. (*Obsolète, voir* RFC4301)

7.2 Références pour information

[RFC2402] S. Kent et R. Atkinson, "En-tête d'authentification IP", novembre 1998. (*Obsolète, voir* RFC4302, 4305)

[RFC2406] S. Kent et R. Atkinson, "Encapsulation de charge utile de sécurité IP (ESP)", novembre 1998. *(Obsolète, voir* RFC4303)

[RFC2408] D. Maughan, M. Schertler, M. Schneider et J. Turner, "Protocole Internet d'association de sécurité et gestion de clés (ISAKMP)", novembre 1998. *(Obsolète, voir la* RFC4306)

[RFC2409] D. Harkins et D. Carrel, "L'échange de clés Internet (IKE)", novembre 1998. *(Obsolète, voir la* RFC4306)

[SPP] Sanchez, L. and M. Condell, "The Security Policy Protocol", *Travail en cours*.

8. Déclinatoire de responsabilité

Les vues et spécifications présentées ici sont celles des auteurs et ne sont pas nécessairement celles de leurs employeurs. Les auteurs et leurs employeurs déclinent spécifiquement toute responsabilité pour tout problème découlant de la mise en œuvre ou utilisation correcte ou incorrecte de la présente spécification.

9. Remerciements

Les auteurs remercient les membres du groupe de travail IPsec Policy qui ont contribué au présent document.

10. Adresse des auteurs

Matt Blaze
AT&T Labs - Research
180 Park Avenue
Florham Park, NJ 07932
USA
mél : mab@crypto.com

Angelos D. Keromytis
Computer Science Department
Columbia University
1214 Amsterdam Avenue, M.C. 0401
New York, NY 10027, USA
mél : angelos@cs.columbia.edu

Michael C. Richardson
Sandelman Software Works Corp.
470 Dawson Avenue
Ottawa, ON K1Z 5V7 Canada
téléphone : +1 613 276-6809
mél : mcr@sandelman.ottawa.on.ca

Luis A. Sanchez
Xapiens Corporation
PO Box 9023694
San Juan, PR 00902 USA
téléphone : +1 (787) 832-4717
mél : lsanchez@xapiens.com

11. Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d'édition des RFC est actuellement fourni par la Internet Society.