Title: Linux Kernel におけるIPsec
Author(s): usagi-core@linux-ipv6.org
Date: 02/09/2005

-- 目次

-- 本文

1 IPsec 概要

IPsec は、IP を用いた通信に対してIP レイヤで機密性、完全性、認証といったセキュリティサービスを提供する。このため既存のアプリケーションに手を加えることなくセキュリティサービスを提供できるという利点を持つ。IPsec の構成は、大きく二つに分けることができ、一つは、パケットを処理する機能であり、もう一つは、パケットを処理するた
めに必要な共有鍵や鍵の有効期限などを交換する機能である。IPsec には、Authenticaiton Header(AH)とEncapsulating Security Payload(ESP)があり、それぞれにトンネルモードとトランスポートモードが定義されている。

2 Linux におけるIPsec

Linux では、パフォーマンスの観点からIPsec のパケット処理はカーネル内に実装され、鍵交換はデーモンとしてユーザランドに実装される。ユーザランドとカーネル間のインターフェースはKAME と互換性のあるPF_KEYv2(RFC2376)に独自の拡張を加えたものとnetlink socket によって実装され、どちらのインタフェースを使ってもセキュリティポリシとIPsec SA の設定ができる。
Linux のIPsec は、Linux-2.4 までは、FreeS/WAN プロジェクト(http://www.freeswan.org/)によってパッチという形で提供されてきた。しかし、Linux-2.5 からはカーネルメンテナによってFreeS/WAN とは異なる独自のアーキテクチャを用いたIPsec がメインラインカーネルに取り込まれている。このため最新の安定板であるLinux-2.6 からはUSAGI Project で行ったIPsec のIPv6 サポートと合わせではカーネルをビルドする際に設定だけことでIPv4,IPv6 の両方でIPsec の機能を使用することができる。

3 鍵交換デーモン

鍵交換デーモンに関しては、Linux に対応したracoon がipsec-tools プロジェクトから提供されており、使用することができる。また、FreeS/WAN の後継プロジェクトであるOpenS/WAN (http://www.openswan.org)からは、Linux-2.6 に対応したIKE デーモンpluto が提供されている。
また、IKE の次期バージョンであるIKE version 2(IKEv2)や認証にKerberos を用いた鍵交換プロトコルKINK をサポートする鍵交換デーモンをWIDE プロジェクトのIPsec ワーキンググループで開発しており、これもLinux-2.6 をサポートする予定である。

4 xfrm とstackable destination

Linux-2.6 では、IPsec を実装するにあたり、xfrm とstackable desination というアーキテクチャが導入されている。
xfrm は、xfrm_policy,xfrm_tmpl,xfrm_state 構造体からなり、パケット処理のポリシと実際の処理に必要な情報を分離して管理する構造である。IPsec では、xfrm_policy がセキュリティポリシに相当し、xfrm_state がIPsec SA に相当するように実装されている。xfrm_policy とxfrm_state の関連付けは、xfrm_tmpl によって行われる。
入力処理は、パケットを処理するために先にxfrm_state が検索され、使用されたxfrm_state は、skb のsec_path に保持される。セキュリティポリシとのマッチングはそれらをxfrm_policy の持つxfrm_tmpl と比較することで行われる。

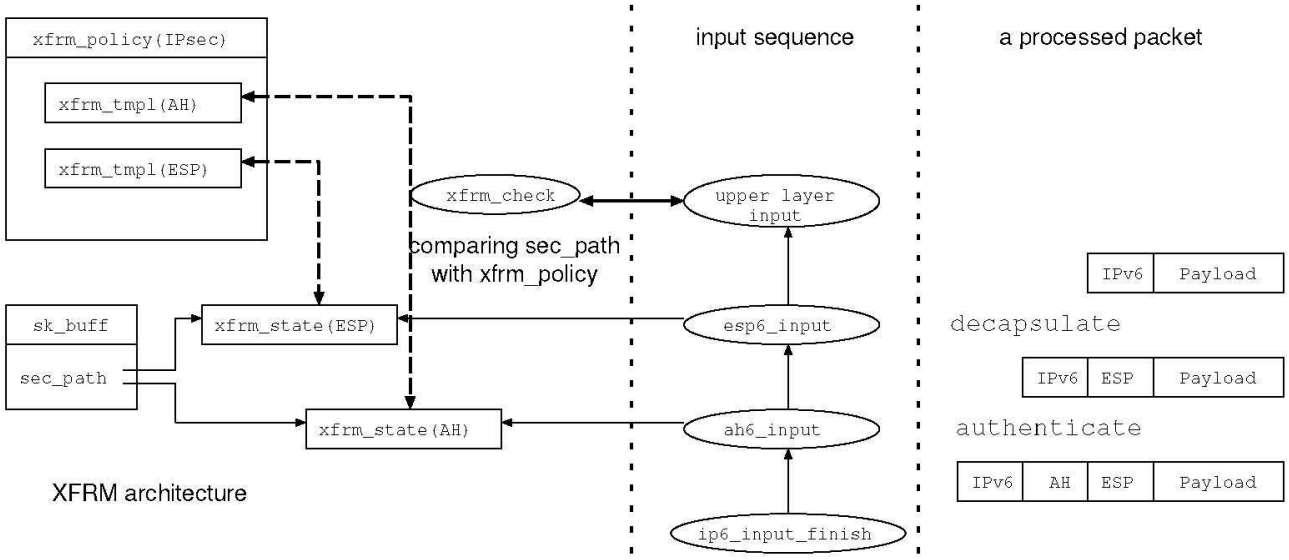

図 1 IPsec の入力処理

stackable destination は、出力処理を効率化するための仕組みで、ルーティングテーブル内で最終的な送信先を示す dst_entry 構造体をスタック構造にし、その出力関数(output)を順次呼び出すことで実現されている。dst_entry の output は、通常パケットを送信する処理にあたり、dst_entry の output を呼び出す時点で IP ヘッダを含むパケットは完成している。IP パケットのフラグメント処理はさらにこの後に行われる。

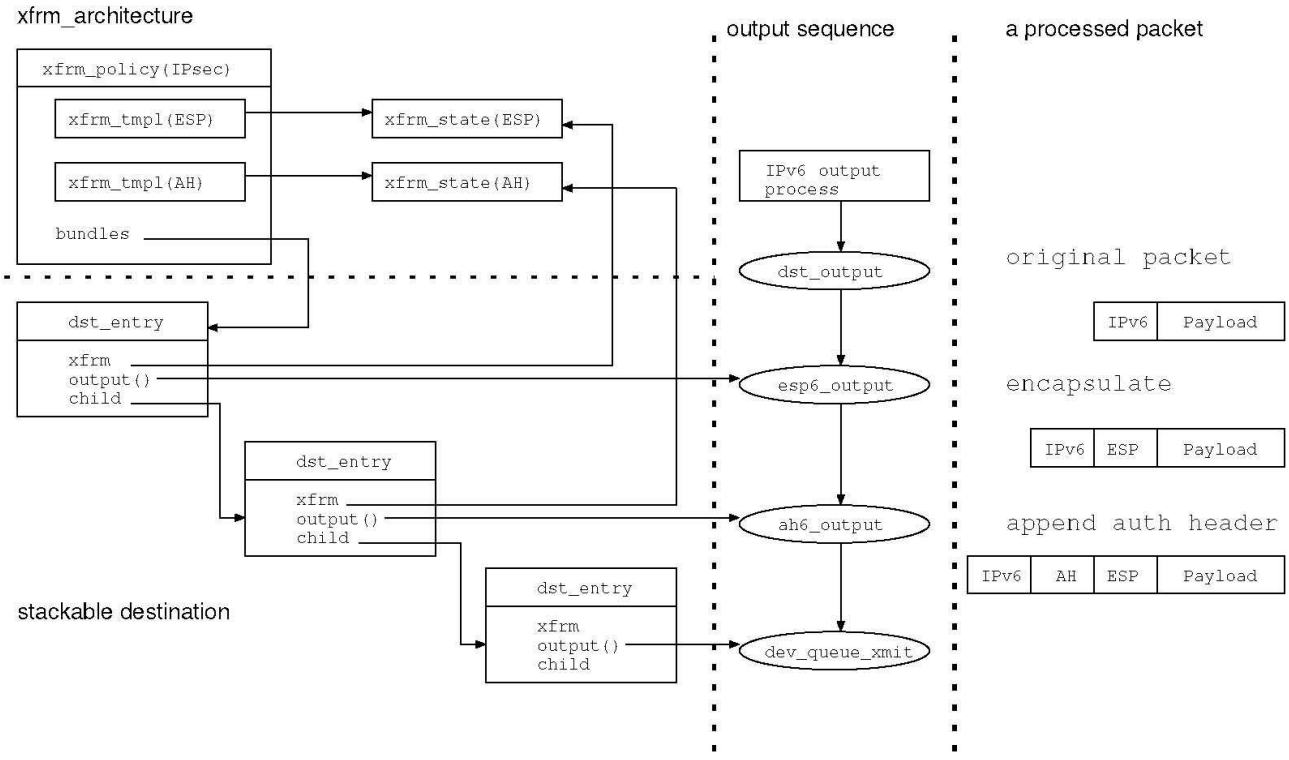

図 2 IPsec の出力処理

5 カーネルでの Mobile IPv6 サポート

Mobile IPv6 の実装にあたっては、RFC3776 にあるように、Mobile IPv6 のシグナリングを IPsec によって保護する必要がある。Mobile IPv6 のシグナリングにおいて、IPsec の保護を必要とするの

は、Mobile Node(MN)とHome Agent(HA)間で行なわれるHome RegistrationとMobile NodeとCorrespondent Node(CN)間で行われるRouting Optimizationである。仕様では、Home RegistrationをMN-HA間のトランスポートモードで保護し、Routing OptimizationをMN-HA間のトンネルモードで保護する。

USAGI Projectでは、Mobile IPv6を上記のxfrmとstackable destinationを用いて実装している(Mobile IPv6については、2.1を参照)。このため、Mobile IPv6に対してIPsecを適用するためには、Mobile IPv6とIPsecの両方から使用されるxfrm_policyと、xfrm_stateを検索する際のパラメータを保持するxfrm_tmplを適切に保つ必要がある。

現在の実装では、Mobile IPv6を管理するmipdが、Mobile IPv6の処理に必要なxfrm_policyとxfrm_stateに加え、それらを保護するために必要なIPsecのためのxfrm_policyとxfrm_stateを設定する。この設計は、Mobile IPv6関連の設定が一元化されるという利点もある。しかし、一方でユーザーが設定したセキュリティポリシによってMobile IPv6のパケットが思わぬ影響を受けてしまうことも考えられる。特にCNとの通信では、MN-HA間のトンネルSAに加えてMNのHome AddressとCN間にもIPsecを設定する可能性がある。このような設定では、(1)MNのHome AddressとCNのアドレス間のトンネル、(2)MNのCare of AddressとHA間のトンネルを正しい順序でパケットにて供する必要がある。そのため今後は、Mobile IPv6の設定とIPsecの設定を設定時にカーネル内で正しい順序でマージするような設計に変更する予定である。

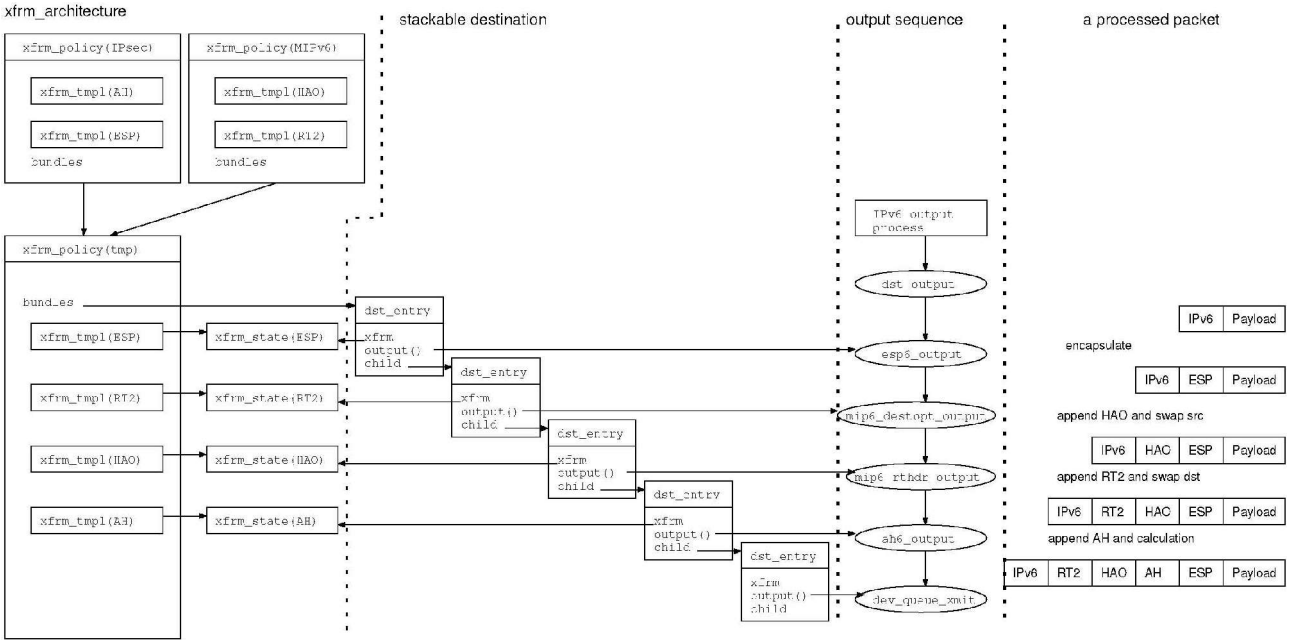

図3 MIPv6のxfrm_policyとIPsecのxfrm_policyのマージ