エンドポイント間のポリシーに基づくVPN構築方式

4H－04

萬木優子　原田道明　高野啓　金枝上敦史
三菱電機(株)情報技術総合研究所

1．はじめに

ネットワークの品質、安全性への要求が高くなるのに伴って煩雑化しているネットワーク管理の負荷を軽減するために、ネットワーク装置の設定を抽象的に記述できるポリシーを用いたネットワーク管理が普及してきている。

IETFのポリシーワークグループが標準化を進めているPCIMe[1]は、各種ネットワーク装置に対する設定を装置の実装に依存しないポリシーとして記述するためのポリシー管理モデルを規定している。対象装置はQoS、IPsec装置[2]、ファイアウォール、NAT装置等に拡張されている。

QoSやファイアウォールの設定では、1つの装置が1つのサイトを担うため、ポリシーと実際の設定の対応が取りやすい。一方VPN(Virtual Private Network)では、VPN経路上に存在する少なくとも2つのVPN終端を含む各種の機器を統合的に管理する必要がある。

今回、PCIMeのポリシー管理規格に準拠しつつVPNの管理負荷を削減することを目指し、管理者がエンドポイントに着目してVPNを管理するための方法を検討したので報告する。

2．IPsecによるVPN構築の特徴

IPsecによるVPNにはいくつかの形態があるが、いずれの形態でもIPsecプロトコルを実装する2つの装置間の通信が秘匿される。IPsecを実装する装置は通信のエンドポイント(ユーザが直接操作するPCやアクセス先のサーバ等、通信の末端装置）と必ずしも一致せず、次のような形態が一般的である。それぞれの形態のVPN構築における特徴を述べる。

(1)サイト間VPN

2つのサイトの入口に置かれたVPNゲートウェイ間にVPNを構築する。エンドポイントからゲートウェイまでの領域はLAN等の安全な領域と考えられる。VPN装置がファイウォールを兼ねるか、VPN装置がファイアウォールの内側に置かれる場合が多い。VPN装置がファイアウォールの内側に置かれる場合、ファイアウォールにIPsecを通過させる設定が必要である。

VPN Configuration based on End-to-End Policy
Yuko YURUGI, Michiaki HARADA, Akira TAKANO,
Atsushi KANAEGAMI
INFORMATION TECHNOLOGY R&D CENTER
MITSUBISHI ELECTRIC CORPORATION

(2) リモートアクセスVPN

ノートPC等の移動端末や自宅等から特定のネットワークにアクセスする場合に用いられる形態で、アクセス先のネットワークの入口(アクセスサーバ)でユーザ認証やIPアドレスの割り当てが行なわれたのち、端末からアクセスサーバまでの間がVPN接続される。この形態におけるVPN構築では、VPN装置の設定以外に、アクセスサーバに対しユーザ認証やアドレス割り当ての設定が必要となる。

上記のいずれの形態においても、VPNの構築には以下のような特徴がある。

・2つのVPN装置が連携して動作するよう対称的な設定が必要である。

・VPN装置以外にも経路上の関連装置に対する設定が必要である。

3．VPNに適したポリシー管理

PCIMeは、基本的にネットワーク装置単体に対する設定を抽象化する表現方式である。ファイアウォール装置は、1台の装置が1つのサイトを保護する目的で置かれることが多いため、管理者の関心であるセキュリティポリシーと装置設定を1：1に対応させやすくPCIMeの表現方法が適している。

一方、IPsecプロトコルによるVPNでは、2章で述べたようにVPNの両側にある2台の装置が連携して動作する必要があり、通常2台の装置に対し、暗号化アルゴリズムやタイムアウト時間等に関して同一の設定が行われる。

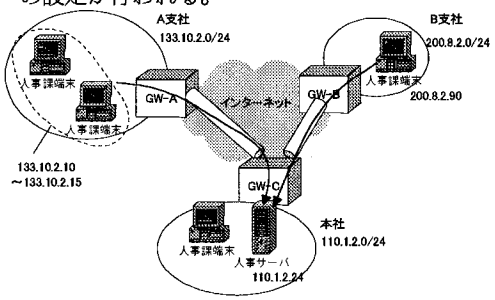

図1：ポリシー適用先ネットワーク構成例

例えば、図1のネットワーク構成において支社A，Bの人事課端末から本社の人事サーバへのftpアクセスを許す場合、GW-A，GW-Bには各サイト内人事端末から本社人事サーバへ出て行くftpパケットを暗号化する設定が、GW-CにはGW-A，GW-BからのVPNアクセスを受諾するための設定がなされる。

しかし管理者にとって関心があるのは、支社の人事端末と本社の人事サーバの間で行なわれるVPN通

信の内容であり、個々の装置の設定はそのための手段に過ぎない。従って、PCIMeのように個々の装置のポリシーを直接表現するのではなく、複数装置の連携によるVPNとしての動作を表現できる方が管理者にとって望ましいと考えられる。

そこで、我々はVPNポリシーをエンドポイント間のポリシーとして表現する方法を検討し、現在GUI上でエンドポイント間のポリシーを定義することによって個々の装置の設定を生成するシステムを試作中である。以降でこのシステムの実現方式について検討した内容を説明する。

4．エンドポイント間ポリシー管理の実現検討

4.1．ポリシーの表現

ポリシーは条件とアクションから構成され、条件には受信したトラフィックの内容や方向等が、アクションには条件に適合したトラフィックの扱い方が定義される。表1は、図1におけるA支社のGW-Aに対するポリシーの記述例である。

表1：装置ポリシー

順位	条件				アクション
	方向	発信元アドレス	宛先アドレス	サービス	
1	out	133.10.2.10～133.10.2.15	110.1.2.24	ftp	IPsec*
2	out	133.10.2.10～133.10.2.15	110.1.2.24	any	廃棄

*IPsecアクションにはさらに詳細に暗号化方式等が指定される。[2] [3]

VPNは、図1のように3つ以上のエンドポイントから構成される場合もあるが、この場合も2つのエンドポイント間のVPNの組み合わせであり、エンドポイント間ポリシーは2つのエンドポイント間の条件を記述できれば良い。同一ポリシーを複数の実エンドポイントに適用可能とするため、エンドポイントをパラメータ化した表2のような表現方法とした。

表2：エンドポイント間ポリシー

順位	条件			アクション
	エンド1	エンド2	サービス	
1	拠点A人事課	人事サーバ	ftp	IPsec
2	拠点A人事課	人事サーバ	any	廃棄

4.2．ポリシー実行方式

次に、前節表2のようなエンドポイント間ポリシーから表1のような装置別ポリシーへの変換を自動的に行なうための仕組みを検討した。

PCIMeでは、ポリシーに、そのポリシーを適用すべき装置の"役割"が対応付けられる。実際の装置には装置の機能に一致する役割を割り当てることで、個別にポリシーを定義することなく、役割に対応したポリシーが自動的に適用される仕組みである。ポリシー定義量を抑制するためにエンドポイント間ポリシーについても同様の仕組みが必要である。

VPNの構築では、前述のようにVPNの利用形態によって経路上で設定対象となる装置の種類が決まるため、経路上の装置の並びを抽象化したモデル（以下、経路モデル）に対応してポリシーを定義するというアプローチが考えられる。経路モデルは、各装置への設定内容が各装置の役割およびVPN経路上の相互の位置によって決定することからこれらを表現するものとする。例えば、サイト間VPNの経路モデルは図2のように定義される。

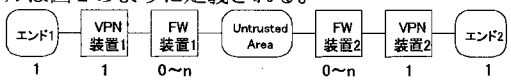

図2：サイト間VPNの経路モデル

この経路モデルに対応して、エンドポイント間ポリシーからPCIMeに準拠した装置ポリシーを生成するための生成規則を定義する。生成規則には表3のように、エンドポイント間ポリシーの方向とアクションに対し、生成すべき各装置ポリシーを定義する。

この規則を図1のネットワークに適用したとするとGW-A,GW-BにVPN装置1のポリシーが、GW-CにVPN装置2のポリシーが適用される。

表3：装置ポリシー生成規則(発信元/宛先アドレス省略)

生成対象 / 方向 / アクション	VPN装置1	FW装置1	FW装置2	VPN装置2
エンド1→2 IPsec	方向:out サービス:ftp ｱｸｼｮﾝ:IPsec	out IPsec 透過	in IPsec 透過	in ftp IPsec
エンド1→2 廃棄	方向:out サービス:any ｱｸｼｮﾝ:廃棄	(追加設定なし)	(追加設定なし)	in any 廃棄
…	…	…	…	…

これにより経路モデルのエンドポイントや経路上の装置が実装置群に割り当てられることによって各装置に設定すべきポリシーが決定する。

4.3．今後の検討課題

・トポロジー情報の利用－適用先ネットワークのトポロジー情報から経路上の装置を自動検出することが可能である。これにより管理者が業務に直接関係するエンドポイントの管理に集中できるようになる。

・複数のエンドポイント間ポリシーの共存－同一ネットワークに複数の利用形態のエンドポイント間ポリシーが適用される可能性がある。複数ポリシー間の優先順位付け機能、矛盾検証機能等が必要である。

5．まとめ

VPN構築に際し、エンドポイント間のVPNポリシーからVPN経路上の複数の設定対象装置に設定を行うための方法を示した。この方法によりネットワーク管理者は、1つのVPNを1つのエンドポイント間ポリシーによって定義することが可能となる。

現在、我々は本方式の基本機能の試作を行なっており、今後も実用化に向けた機能検討を継続していく予定である。

[参考文献]

[1] http://www.ietf.org/internet-drafts/draft-ietf-policy-pcim-ext-06.txt, "Policy Core Information Model Extentions"

[2] http://www.ietf.org/internet-drafts/draft-ietf-ipsp-config-policy-model-04.txt, "IPsec Configuration Policy Model"

[3] http://www.ietf.org/internet-drafts/draft-ietf-ipsp-ipsecpib-03.txt, "IPSec Policy Information Base"