Floyd-Hoare論理を応用したVPN構築のための経路設定支援

善明 晃由
株式会社 東芝 研究開発センター

VPNの構築は、対象システムの構成を把握した上で、VPN自体の設定に加えてルーティングなどの様々な種類の設定を行う必要があるため、ネットワークに関する専門知識を要求する困難な作業となる。本稿では、VPNを利用する際に必要となる様々な種類の設定を、Floyd-Hoare論理に倣った推論を用いて導出する方法を提案する。提案する方式は、様々な種類の設定をパケットの状態を遷移させる作用として統一的にモデル化することで、ルーティングやVPNなど、様々な種類の設定を同時に導出することができる。また、複数のサブシステムが協調しながら、サブシステム毎に必要となる設定を導出することで、システム構成を一元的に把握することなく、VPNを利用する際に必要な設定を導出することができる。

Supporting Routing Configurations for VPNs using Inference based on Floyd-Hoare Logic

Teruyoshi Zenmyo
Corporate Research & Development Center, Toshiba Corporation

Construction of a VPN is a difficult task since it requires various types of configurations and understanding of target system's network structures. This paper proposes a technique to support construction of VPNs by deriving needed configurations based on Floyd-Hoare Logic. The proposed technique achieves an integrated support for VPNs configurations with unified models in which various types of configurations(e.g. routing, VPN tunneling) are represented as operations to packets. Additionally, multiple sub-systems collaborate for deriving needed configurations without centralized management of overall network structure. Each sub-system derives needed configurations related to the sub-system, and then requests remaining derivation to an appropriate sub-system.

1 はじめに

現在、インターネットを介して情報システムを接続する方法として、IPsecなどのインターネットVPN（以下、単にVPNと呼ぶ）が注目されている。

VPNは、専用線に比べて低コストであるなどのメリットがある。しかし、VPNの構築は、ネットワークに関する専門知識を必要とする困難な作業である。これは、IPsecなどのVPNプロトコル自体が複雑なことに加え、状況によっては、ルーティングテーブルなども併せて設定する必要があるためである。また、VPNを導入するシステムのシステム構成を正しく把握しておく必要もある。そこで、VPNを構築するための設定を支援することが必要となる。

VPN構築支援においては、VPNやルーティングなどの設定を統合して扱う必要がある。これは、VPN構築において、VPNの設定のみを支援するだけでは不十分であり、前述のように、VPNの設定に加えルーティングテーブルの設定などを併せて設定する必要があるためである。

また、VPNを用いて複数の情報システムを接続する際には、それらのネットワーク構成を分散管理できることが要求される。複数のシステムのネットワーク構成を集中的に管理する場合、管理する情報が膨大になるという問題があるためである。また、セキュリティ上の理由等により、接続先システムのネットワーク構成が把握できない可能性もある。

本稿では、Floyd-Hoare論理[3]を応用することでサブシステム毎に必要な設定を導出する方式を提案する。提案方式において、VPNや経路設定など

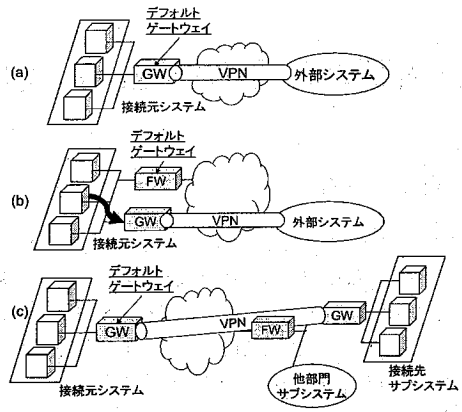

図 1: VPN のバリエーション

のネットワーク機器の設定は、パケットへの作用として統一的にモデル化される。したがって、様々な種類の設定に関して統合された支援が可能となる。また、各サブシステムは、ネットワーク設定要求を受けると、自サブシステムに関する設定を導出する。その際に、自サブシステム以外のネットワークに関する設定は、他のサブシステムに要求することによって、複数のサブシステムの構成を一元的に把握することなしに、必要な設定を導出できる。

2 VPN 構築支援への要件と本研究の目的

本節では、VPN の構築を支援する際に必要となる要件について述べる。VPN 構築においては、以下の３つの課題がある。

- VPN 自体の設定が複雑である。
- VPN 設定に付随する他の設定 (例えば、ルーティング情報など) を行う必要がある。
- 複数の組織を接続するため、全システム構成を一元的に把握できない可能性がある。

図１は、VPN を利用する際のシステム構成の例を示したものである。本節では、図１で示す VPN を構築する際に必要となる設定について考える。

まず、図 1(a) における VPN は、接続元システムのデフォルトゲートウェイである GW に VPN 設定を行い、外部システムとの接続を実現している。この際には、VPN 自体の設定に対する支援が必要である。

次に、図 1(b) における VPN について考える。図 1(b) では、接続元システムと外部ネットワークとの境界にファイアウォール (FW) と GW が存在している。また、接続元システムのデフォルトゲートウェイは、VPN の終端でない FW に設定されている。この場合、図 1(a) と同じ設定では不十分である。これは、図 1(b) の接続元システムにおけるデフォルトゲートウェイが FW であるため、VPN を通過すべきパケットも FW にルーティングされてしまうためである。つまり、図 1(b) の VPN を構築する際には、VPN 自体の設定に加えて付随するルーティング情報の設定も同時に支援される必要がある。

図 1(c) では、外部システムが複数のサブシステムから構成されている。この場合、外部システムにおいてルーティングや FW のフィルタリングルールなどの設定が必要となる可能性がある。しかし、セキュリティ上の理由や外部システムの構成変更などにより、接続元システムが、図 1(c) の VPN を利用するために必要な設定を把握できない可能性がある。

VPN 自体の設定に関しては、IPsec の設定検証 [1][2] などの研究がなされている。しかし、いずれも VPN に付随する設定までは対象としてない。このため、例えば、図 1(b) のルーティング情報の設定などの VPN に付随する設定の洩れが VPN 通信が失敗する原因である場合、その検出、修正が困難となる。

そこで、本研究では、VPN とそれに付随する設定を同時に支援することを目的とする。また、本研究では、図 1(c) の状況にも対応可能なように、システム構成を一元的に把握できない状況での VPN 設定支援を考える。

3 推論による VPN 設定支援

本節では、VPN を用いて複数のサイトを接続する際に必要となる設定を推論を用いて導出する方法を提案する。

提案する方式では、通信の仕様を Floyd-Hoare 論理 [3] に倣い、パケットの事前状態、事後状態と通信経路によって記述する。なお、この形式で記述した仕様を通信仕様と呼ぶことにする。また、情報シス

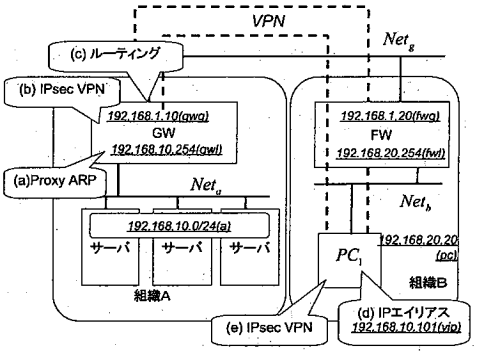

図 2: VPN のための設定例

テムのシステム構成とネットワーク上に存在する通信機器が実現可能な設定をモデル化しておく。設定とは VPN の符号化、復号化やルーティングテーブルなどである。ここで、設定は、パケットの状態を遷移させるパケットへの作用としてモデル化する。

提案する方式は、対象の情報システムにおいて、パケットが通信仕様に指定された事前状態から、事後状態へ遷移可能かを推論することによって、必要となる設定を導出する。この推論の際に利用された作用を、要求された通信を実現されるために必要な設定と見なす。

さらに、各サブシステムは、自サブシステムが管理する通信経路において必要となる設定のみを導出し、管理対象外の通信経路においては、他のサブシステムに推論を要求する。これにより、VPN を用いて接続する全てのサブシステムの構成を把握することなく、各サブシステム毎に必要な設定を導出することができる。

本節では、図 2 に示す VPN を設定する場合を例に、提案するネットワーク設定支援方式を説明する。図 2 は、組織 B 内の PC を組織 A 内に存在するように仮想化することを目的とした VPN を実現するための設定を示している。

また、以下を仮定する。

- VPN プロトコルとして、IPsec を用いることと、暗号化や鍵交換の方式については、事前に決められているものとする。また、IPsec の機能を持つ計算機は、GW と PC_1 のみとする。
- 組織 A は、組織 A のシステム構成、および、FW の外部側インタフェース fwg と PC_1 のインタフェース pc が、GW インタフェース gwg から到達可能であることを把握している。その他の組織 B のシステム構成については情報をもたない。
- 組織 B は、組織 B のシステム構成、および GW の外部側インタフェース gwg が FW のインタフェース fwg から到達可能であることを把握している。その他の組織 A のシステム構成については情報をもたない。

3.1 通信とネットワークのモデル

ここでは、提案方式におけるネットワークと通信のモデルについて述べる。

3.1.1 通信仕様の記述

ここでは、通信仕様に記述すべき項目を検討する。

インターネットなどのネットワークにおける通信は、パケットを、パケットの送信元の計算機から、宛先として指定された計算機に到達させる必要がある。そこで、通信の仕様には、パケットの送信元と宛先を記述する必要がある。

また、パケットの内容に変更がなされる場合がある。例えば、VPN トンネルを利用する場合は、VPN トンネルの入口でパケットの送信元、宛先アドレスがトンネル用のアドレスによってカプセル化され、VPN トンネルの出口で元のアドレスに復号化される。パケットのアドレスによって、例えば、次のルーティング先など、通信機器がパケットに与える作用が変化する。そこで、パケットが、どのようにカプセル化されているかを記述できる必要がある。

さらに、通信経路についても記述できる必要がある。これは、例えば、図 1(b) の状況では、利用する GW を指定する必要があるためである。

そこで、提案方式では、通信仕様に以下の情報を記述する。

- パケットの事前条件
- 通信経路
- パケットの事後条件

図 2 の VPN の通信仕様 ($Spec$) を以下に示す。

$\{(a, vip), a\}$
$Net_a; GW; Net_g; FW; Net_b; PC1$
$\{(a, vip), pc\}$

1 行目と 3 行目は、それぞれパケットの事前条件と事後条件を示す。小括弧中の値は、それぞれパケットの送信元アドレスと宛先アドレスである。小括弧外の値は、パケットが存在する位置である。例えば、$\{(a, vip), pc\}$ は、送信元アドレスが a(192.168.10.0/24) であり、宛先アドレスが vip(192.168.10.101) のパケットが PC_1 のインタフェース pc に存在することを示す。また、VPN トンネルにおけるアドレスフィールドのカプセル化を表現するために、アドレスはスタックを用いて表現するものとする。(例えば、宛先 pc のパケットにカプセル化する場合は $pc(vip)$ とする。)

2 行目には通信経路が指定されている。すなわち、前述の通信仕様は、送信元アドレスが a、宛先アドレスが vip のパケットが、Net_a、GW、Net_g、FW、Net_b、PC_1 を経由し、PC_1 上のインタフェース pc まで到達することを指定している。

ここで、前記の通信仕様 $Spec$ は、それを記述するために全てのシステム構成を把握しておく必要があるため、組織 A、または組織 B の持つ情報だけでは記述できない。このため、例えば組織 A から図 2 に示す VPN 構築を要求する場合は、組織 B の管理下にあるシステムに仮の経路名を指定して、下記のように記述する。なお、下記の通信仕様を $Spec_A$ とする。

$$\{(a, vip), a\} Net_a; GW; Net_g; Sys_B \{(a, vip), pc\}$$

3.1.2 パケットの状態遷移

ここでは、送信されたパケットが目的の計算機へ到達するまでの、パケットの状態遷移について考える。パケットは、送信された後、目的の計算機に到達するまでに、以下の 2 種類の状態遷移をする。

- ある計算機のインタフェースから他のインタフェースへ移動する。
- パケットの内容が変化する。これは、VPN トンネルを利用する際のアドレスフィールドのカプセル化などである。

上記 2 種類の状態遷移は、通信経路上に存在するネットワーク機器になされた設定によって決定される。したがって、ネットワーク機器になされる設定をパケットの状態を遷移させるパケットへの作用と考えることができる。2 種類の状態遷移をネットワーク機器のパケットへの作用として統一して扱うことによって、VPN を利用する際に必要となる様々な種類の設定を同時に扱うことができる。

以下に、本稿で用いるネットワーク機器のパケットへの作用を示す。

- $route(if_1, Net, src, dst, if_2)$: インタフェース if_1 を持つネットワーク機器は、if_1 からネットワーク Net を介して、送信元アドレス src、宛先アドレス dst を持つパケットをインタフェース if_2 へルーティングできる。
- $receive(if, Net, src, dst)$: インタフェース if を持つネットワーク機器は、ネットワーク Net を介して、送信元アドレス src、宛先アドレス dst のパケットを if で受信できる。
- $enc(Node, src_1, dst_1, src_2, dst_2)$: ネットワーク機器 $Node$ は、送信元アドレス src_1、宛先アドレス dst_1 を持つパケットを、送信元アドレス src_2、宛先アドレス dst_2 を持つパケットに符号化できる。
- $dec(Node, src_2, dst_2, src_1, dst_1)$: ネットワーク機器 $Node$ は、送信元アドレス src_2、宛先アドレス dst_2 を持つパケットにカプセル化されたパケットを、復号化することができる。

3.1.3 ネットワークモデル

ここでは、要求される通信仕様の実現可能性を推論する際に用いるネットワークモデルについて述べる。

まず、ネットワークモデルには各ネットワーク機器の物理的な接続関係に関する情報が必要である。ネットワーク機器は、ネットワークインタフェース(以降、単にインタフェースと呼ぶ) を介してネットワークと接続される。ここで、ネットワークとネットワーク機器をインタフェースの集合と考えると、各ネットワーク機器の接続関係は以下のように定義できる。

ネットワーク機器 N_1 と ネットワーク機器 N_2 がネットワーク NW_1 を介して接続されている。
$\Rightarrow \exists if_1 \in N_1, if_2 \in N_2.(if_1 \in NW_1 \wedge if_2 \in NW_1)$
(ただし、if_1、if_2 はインタフェース)

次に、各ネットワーク機器においてどのような設定が可能かを把握する必要がある。ここで可能な

設定とは、ネットワーク機器が持つ機能、または、システムの運用ポリシーなどによって制限される。3.1.2 節に述べたように、ネットワーク機器の設定はパケットの状態遷移に影響する。そこで、各ネットワーク機器 (N) において可能な設定を、N から N がパケットに与えることが可能な作用の集合 OP への関数 f としてモデル化する。

また、作用としてモデル化された設定は、その設定を実際に行うための方法と関連づけておく。例えば、Linux がインストールされた計算機をゲートウェイとして用いる場合は、作用 *route* と route コマンドによるルーティングテーブルの設定方法を関連づけておく。

3.2 推論規則

通信仕様に記述される通信を実現するためには、経路上に存在するネットワーク機器がパケットに与える作用によって、パケットが通信仕様に指定される事後状態まで遷移する必要がある。すなわち、要求された通信仕様の実現可能性を判定するには、与えられたシステムにおいて、通信仕様に指定された事前条件から事後条件までの遷移が可能であることを証明すればよい。

ある作用を適用することによって、パケットの存在位置が通信経路上の次の要素 (e とする) に進むことができた場合、証明すべき通信仕様は、e 以降の経路に関するものになる。すなわち、ネットワーク機器の作用を通信仕様の変換と見なし、再帰的に作用を適用していくことで、与えられた通信仕様が実現可能かを証明することができる。

例えば、3.1.1 節の $Spec_A$ には、事前条件として $\{(a, vip), a\}$ が指定されている。ここで、宛先 vip を持つパケットを通信経路上の次のネットワーク機器 GW のインタフェース gwl が、例えば、ProxyArp の設定をすることによって、受信できるとする。このとき、状態 $\{(a, vip), a\}$ のパケットは、GW 上のインタフェース gwl に移動することができる。すなわち、以下の推論規則が成り立つ。

$$receive(gwl, Net_a, a, vip) \in f(GW) \Rightarrow$$
$$Spec_A \rightarrow$$
$$\{(a, vip), gwl\}GW; Net_g; Sys_B\{(a, vip), pc\}$$

この推論規則は、以下のように一般化できる。

$$receive(if_1, N_1, s, d) \in f(N_2) \wedge if_1 \in N_1 \wedge if_1 \in N_2$$
$$\Rightarrow \{(s, d), if_0\}N_1; N_2; N^*\{(s, d), if_n\} \rightarrow$$
$$\{(s, d), if_1\}N_2; N^*\{(s, d), if_n\}$$

ただし、N^* は、インタフェースの集合 (ネットワーク機器、またはネットワーク) のリストとする。

また、この推論を適用した場合を、以下のように表すことにする。

$$\frac{receive(if_1, N_1, s, d) \quad \{(s, d), if_1\}N_2; N^*\{(s, d), if_n\}}{\{(s, d), if_0\}N_1; N_2; N^*\{(s, d), if_n\}}$$

同様に、他の作用に関しても推論規則を定義することができる。以下に、VPN のカプセル化に関する推論規則を示す。

$$enc(N_1, s, d, s', d') \in f(N_1) \Rightarrow$$
$$\{(s, d), if_0\}N_1; N_2; N^*\{(s, d), if_n\} \rightarrow$$
$$\{(s'(s), d'(d)), if_0\}N_1; N_2; N^*\{(s, d), if_n\}$$

ここで、$(s'(s), d'(d))$ は、送信元アドレス s、宛先アドレス d のパケットが送信元アドレス s'、宛先アドレス d' のパケットにカプセル化されていることを示す。

これらの推論規則を用いることで、例えば、図 3 に示す推論図を得ることができる。図 3 では、推論はまだ完了していないが、推論が完了した場合、推論図の左側に示される作用 ($recv_1$、enc_1 など) に対応する設定を適当なネットワーク機器に行うことで、目的の通信を実現することができる。

3.3 組織を跨ぐ推論

図 3 に示す推論図は、組織 A の持つ情報のみを用いた推論であり、要求された通信仕様が実現可能かの証明は完了していない。これは、図 3 の推論図の最上段に現れる $(\{(gwg(a), pc(vip)), fwg), gwg\}Sys_B\{(a, vip), pc\})$ が、組織 B に関する通信仕様であるため、組織 A の持つ情報では以降の推論を行えないためである。

ここで、図 3 の最上段に現れる $\{(gwg(a), pc(vip)), fwg), gwg\}Sys_B\{(a, vip), pc\}$ ($Spec_B$ とする) は、通信仕様の形式であるため、組織 A は組織 B に $Spec_B$ の実現可能性の証明を要求することができる。組織 B は、組織 B のシステム構成に関する情報を把握しているため、組織 A で利用されていた仮経路名 Sys_B を実際の経路のリスト $FW; Net_B; PC_1$ に変換することができる。また、組織 B は、組織 B の管理下にあるネットワーク機

$$\dfrac{\dfrac{\dfrac{recv_1\quad \{(a,vip),gwl\}GW;Net_g;Sys_B\{(a,vip),pc\}}{\{(a,vip),a\}Net_a;GW;Net_g;Sys_B\{(a,vip),pc\}}\quad enc_1\quad \{(gwg(a),pc(vip))),gwl\}GW;Net_g;Sys_B\{(a,vip),pc\}}{route_1\quad \{(gwg(a),pc(vip))),gwg\}Net_g;Sys_B\{(a,vip),pc\}}\quad route_2\quad \{(gwg(a),pc(vip)),fwg),gwg\}Sys_B\{(a,vip),pc\}}$$

ただし、$recv_1 = receive(gwl, Net_a, a, vip)$、$enc_1 = enc(GW, a, vip, gwg, pc)$、
$route_1 = route(gwl, GW, gwg, pc, gwg)$、$route_2 = route(gwg, Net_g, gwg, pc, fwg)$、

図 3: 組織 A 側での推論

器において可能な設定を把握しているため、$Spec_B$ が実現可能かを推論することができる。

3.4 設定の実行

推論によって要求された通信仕様が実現可能だと判断された場合は、推論の際に利用された作用に関連づけられた設定 (3.1.3 節参照) を、実際に行うことで要求された通信を実現することができる。

例えば、図 3 より、図 2 の VPN を実現するために組織 A で必要な設定は、

- $recv_1$ に対応する設定として、Proxy ARP の設定 (2(a))
- enc_1 に対応する設定として、IPsec の設定 (2(b))
- $route_1$、$route_2$ に対応する設定として、ルーティングテーブルの設定 (2(c))

であることが分かる。

本節の例のように、複数の組織においても設定が必要な場合は、各組織で、推論の際に利用された作用に対応する設定を行うことで、全システム構成を一元的に把握することなく、目的の通信を実現できる。

4 まとめ

本稿では、VPN を利用する際に必要となる様々な種類の設定を、Floyd-Hoare 論理を応用して導出する方法を提案した。提案した方法は、様々な種類の設定をパケットの状態を遷移させる作用として統一的にモデル化することで、ルーティングや VPN など、VPN 構築の際に必要となる様々な種類の設定を同時に導出する。また、提案方式において、各サブシステムは、自サブシステムに含まれるネットワーク機器の設定のみ導出し、管理対象でない部分の設定の導出は、他のサブシステムに要求する。このため、全てのシステム構成を一元的に把握することなく、必要な設定を導出することができる。

今後の課題として、複数の設定候補から適切な設定の選択がある。例えば、VPN を利用する設定と利用しない設定が導出された場合、セキュリティや暗号化処理のオーバヘッドなどを考慮して、適切な設定を選択する必要がある。

他の課題として、導出された設定の検証がある。機器になされている他の設定も考慮して、導出された設定が正当なものであるかを検証する必要がある。さらに、導出された設定が他の通信に与える影響も考慮する必要がある。

参考文献

[1] GUTTMAN, J. D., HERZOG, A. L. and THAYER, F. J., Authentication and Confidentiality via IPsec, the 6th European Symposium on Research in Computer Security(ESORICS 2000) (2000).

[2] HAMED, H., AL-SHAER, E. and MARRERO, W., Modeling and Verification of IPSec and VPN Security Policies, Proceedings of the 13th IEEE International Conference on Network Protocols (ICNP'05) (2005).

[3] HOARE, C. A. R., An Axiomatic Basis for Computer Programming, *Communications of the ACM*, **12**, 10 (1969), 576–583.