動的処理解決プロトコル DPRP の性能評価

鈴木　秀和*，渡邊　晃(名城大学)

Performance evaluation of Dynamic Process Resolution Protocol

Hidekazu Suzuki, Akira Watanabe (Meijo University)

１．はじめに

近年，企業ネットワークにおいて内部犯罪が増加しており，イントラネット内のセキュリティ対策が重要視されている．しかし IPsec に代表される既存のネットワークセキュリティ技術では，イントラネット特有の環境に対応することが難しく導入が進んでいない．そこで我々はイントラネットの特徴に柔軟に対応できるネットワークを構築するために動的処理解決プロトコル DPRP（Dynamic Process Resolution Protocol）を提案している(1).

本稿では DPRP を FreeBSD に実装して性能評価実験を行ったので，その結果について報告する．

２．DPRP の動作概要と実装

DPRP は IP 層で動作するプロトコルで，OS の IP 層を改造することにより実現する．DPRP を実装したホスト型装置を GES，ルータ型装置を GEN という．GEN は配下のサブネットに存在する一般端末を保護する役割を持つ．

DPRP は端末間の通信に先立って図 1 に示す 2 往復のネゴシエーションを行う．1 往復目で通信経路上の GE に予め設定されている情報を取得して，パケットの暗号処理や破棄など通信の処理に必要な動作処理情報を動的に決定する．2 往復目で決定した情報を通信経路上の GE に通知し，各 GE は受信した情報をテーブルに保存する．以後の通信はこのテーブルの情報を元に，パケットの暗号化/復号，透過中継や破棄などを行う．DPRP はシステムの変更や端末が移動する度に実行されるため，ユーザが移動してもネットワーク管理者は設定変更の作業を行う必要がない．

３．性能評価

図 1 に示す環境において，GES1，GEN，GES2 間で実行する DPRP の性能を測定した．各装置のスペックは Pentium4 2.4[GHz]，メモリ 512[MB]で，FreeBSD 5.3-Release に DPRP を実装している．測定項目はパケット送受信時における DPRP の内部処理時間（図 1●部分）と，ネゴシエーションのオーバーヘッド（図 1 [i]），実際の通信が開始されるまでの時間（図 1 [ii]）である．参考のために，同一条件下における IPsec/IKE のオーバーヘッドも測定した．IPsec/IKE には KAME/racoon を用いて，GES1-GES2 間で事前に共通鍵を共有した状態でトランスポートモードの通信を行った．

GES1，GEN，および GES1 における内部処理時間の合計

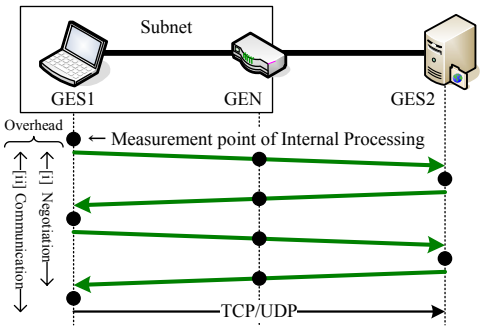


Figure 1.　Test Network and DPRP Negotiation

Table 1.　Overheads of DPRP and IKE

	DPRP	IKE
[i] Negotiation	1,012	1,105,954
[ii]Communication	1,040	2,994,033

Unit : [usec]

は 203.34[usec]であった．オーバーヘッドの測定結果を表 1 に示す．DPRP はネゴシエーション完了後，28[usec]後（[ii]-[i]）に最初のパケットの通信が開始された．一方，IPsec/IKE ではネゴシエーションに約 1 秒，通信が開始されたのはネゴシエーションを始めてから約 3 秒後であった．

IKE はネゴシエーション時に通信を暗号化する際に用いる暗号鍵を公開鍵暗号技術により生成する．DPRP は予め確実な認証の下に配送された暗号鍵を保持しているため，端末間の認証と動作処理情報の生成のみ行うだけでよい．また最初の通信パケットが送信されるまでの時間について，IKE では SA（Security Association）が確立されていないとパケットを破棄するため，TCP の再送処理に頼ることで通信を再開している．一方，DPRP は動作がシンプルであるため，全ての処理をカーネルに実装することができる．そのため IP 層にてパケットを一時的に待避しておき，ネゴシエーション終了時に元に戻すという処理が可能で，高速に通信を再開することができる．

４．まとめ

本稿では DPRP の実装を行い，性能測定を行った．今後は DPRP，IPsec/IKE を利用する場合に発生する管理負荷の評価を行う予定である．

文　献

(1) 鈴木, 渡邊: 情報処理学会研究報告, 2004-CSEC-28, pp.199-204, 2004

動的処理解決プロトコルDPRPの性能評価

Performance evaluation of
Dynamic Process Resolution Protocol

名城大学大学院　理工学研究科

鈴木秀和　渡邊晃

はじめに

- 企業ネットワークにおけるセキュリティ対策の重要性

驚異；不正進入，データの盗聴･改竄，情報漏洩

外部からの驚異

➔ファイアウォール，IDS，通信の暗号化 etc

内部における驚異

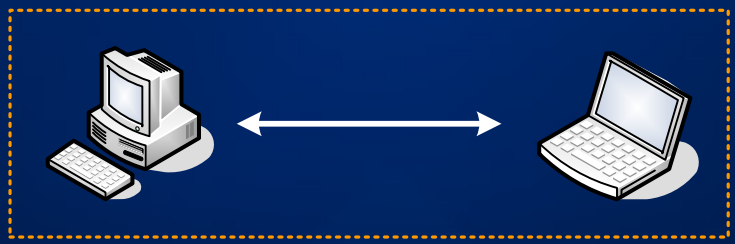
➔ユーザ名とパスワードによる簡単な認証，アクセス制御

通信グループの構築が有効な方法

通信グループの構築

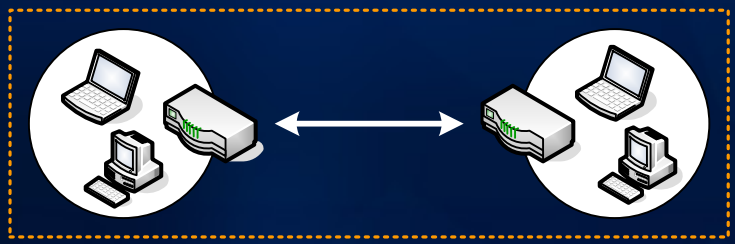
- 通信グループ
  - 同一グループのメンバ間の通信を暗号化
  - 既存のネットワークインフラをそのまま利用可能

個人単位に実現する方式 ➔役職単位でのグルーピングに最適



- IPsecトランスポートモード
- 規模が大きくなると管理負荷も増大

ドメイン単位に実現する方式 ➔部門単位でのグルーピングに最適



- IPsecトンネルモード
- きめ細かい通信グループの定義が困難

柔軟な通信グループを構築するために

イントラネットでは…

- 役職単位や部門単位など複数の通信グループを定義したい
- 部門をまたがって通信グループの定義したい

個人単位/ドメイン単位が混在した方式が望ましい

IPsecは…

- トランスポートモードとトンネルモードの互換性がない
  ➔混在方式の実現は難しい （実現しても管理負荷が大きい）

フレキシブルプライベートネットワーク
FPN (Flexible Private Network)

Flexible Private Network

独自システム

- ネットワークのあるべき姿を示した概念
  - セキュリティと柔軟性を両立

位置透過性

- 端末の位置に影響なく通信グループの関係を維持できる機能

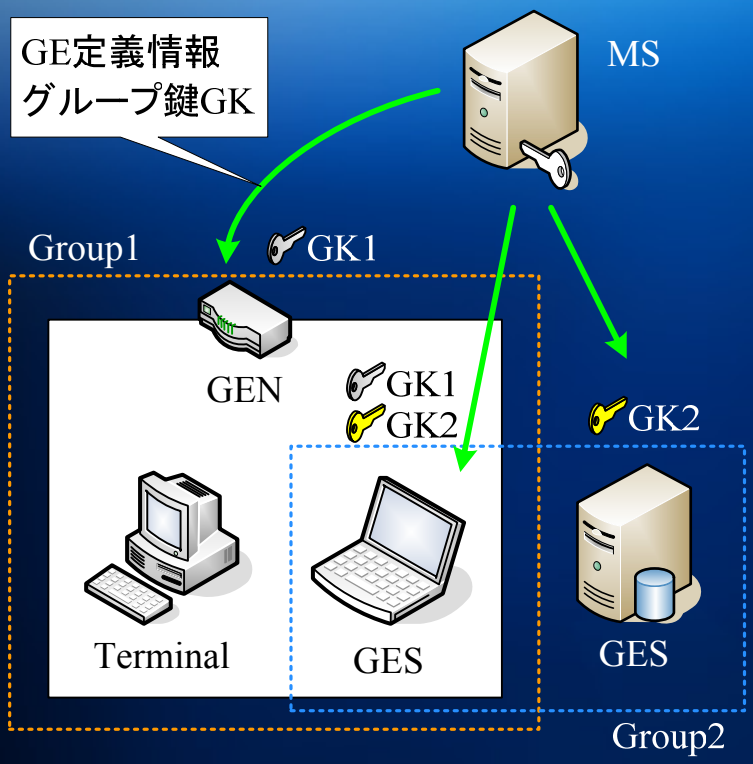
移動透過性

- 通信中に移動してIPアドレスが変化しても通信を継続できる機能

アドレス空間透過性

- IPv4環境におけるグローバル/プライベートアドレス空間の間で自由な双方向通信を実現する機能

FPNにおける通信グループの定義方法

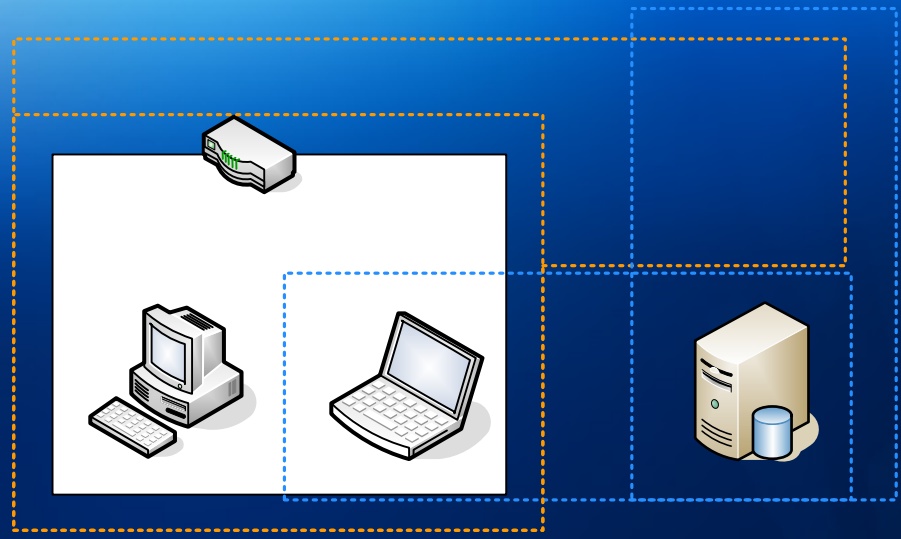


» 構成要素
- GE：通信グループを構成する装置
  - ＞ GES（ホスト型）
  - ＞ GEN（ルータ型）
- MS：グループ管理装置

» MSからGEへ定義情報を配送
- MS-GE間は公開鍵認証
- 同一の秘密鍵（グループ鍵GK）を持つGEの集合を通信グループとして定義
- 通信グループと秘密鍵が1対1の関係

IPアドレスに依存せず，論理的に通信グループの定義が可能

位置透過性



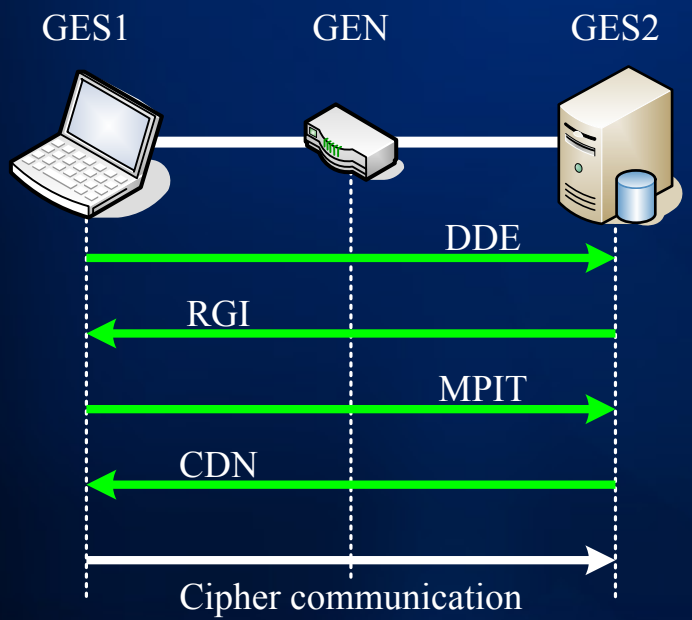
- 位置透過性と暗号化通信を実現するために
  - 通信に先立って通信相手の所属グループを確認
  - 通信パケットの処理に必要な動作処理情報を動的に生成

動的処理解決プロトコル *DPRP*
(Dynamic Process Resolution Protocol)

動的処理解決プロトコルDPRP

提案技術

- 通信経路上の両終端GEと2往復のネゴシエーション
  - グループ定義情報を収集して動作処理情報を決定
  - 決定した情報を通知して動作処理情報テーブルを生成
  - IP層で動作

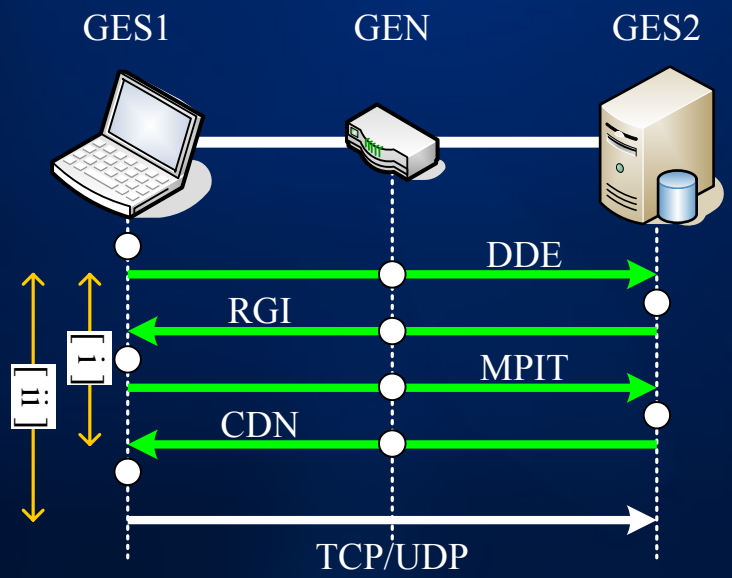


DPRP制御パケット

- DDE (Detect Destination End-GE)
  - 終点GEを検出
- RGI (Report GE Information)
  - 通信経路上の全GEのグループ情報を収集
- MPIT (Make Process Information Table)
  - 決定した動作処理情報の通知と認証
  - 動作処理情報テーブルの生成
- CDN (Complete DPRP Negotiation)
  - DPRPネゴシエーションの終了

DPRPの性能評価実験

- GES1-GES2間のDPRPネゴシエーション
  - 各GEにおけるDPRPの内部処理時間（下図●印部分）
  - DPRPネゴシエーションのオーバーヘッド
    i. ネゴシエーションの時間
    ii. 最初の通信が開始されるまでの時間



スペック（GES1，GES2，GEN）

- Pentium4 2.4GHz
- 512MB
- 100BASE-TX
- OS：FreeBSD 5.3-Release
- KernelにDPRPを実装

性能結果

内部処理時間

単位：μ sec

測定ツール
RDTSC（Read Time-Stamp Counter）

GES1	GEN	GES2	合計
96.59	44.32	62.43	**203.34**

高速に認証と動作処理情報テーブルの生成が可能

オーバーヘッド

単位：μ sec

測定ツール：　Ethereal

	DPRP	IKE
[i]ネゴシエーション	1,012	1,105,954
[ii]最初の通信開始	**1,040**	**2,994,033**

[ii]の結果
DPRP＝約1ミリ秒
IKE＝約3秒

一般の通信にほとんど影響なし

考察1

- ネゴシエーション

DPRP

» 予めMSと公開鍵認証を行い，ネゴシエーション時の認証と通信を暗号化するための共通鍵を取得
→ネゴシエーションは共通鍵暗号処理のみ

IKE

» ネゴシエーション時の認証とは別に通信を暗号化するための共通鍵を生成
→公開鍵技術（DH鍵交換）を利用しているため遅い

考察2

- 一般の通信に対する影響（最初の通信開始）

DPRP

- 実装がシンプルでパケットの待避処理や復帰処理が可能
  →TCPの再送処理は発生しない

IKE

- IKEはアプリケーション層で動作しカーネル（KAME）とリアルタイムに連携できない
  →パケットを破棄してIKEを実行
  →TCPの再送処理に頼っているため遅い（初期RTO＝3秒）

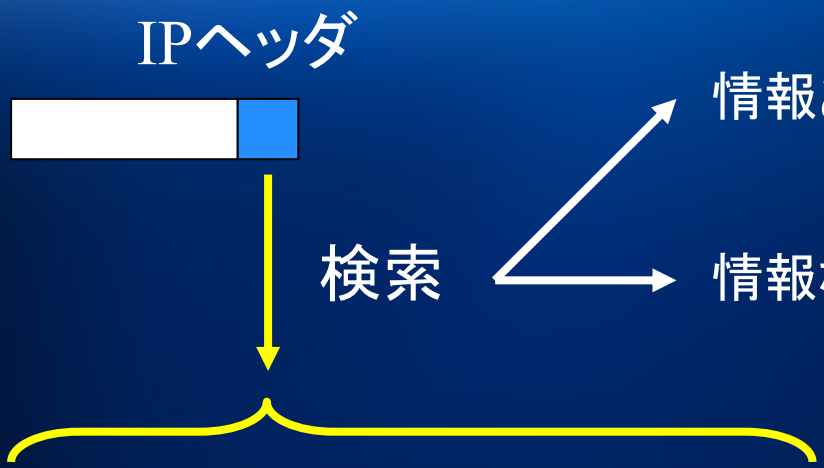
まとめ

- 動的処理解決プロトコルDPRPの性能測定
  - 高速かつ安全に
    - 通信相手を認証することが可能
    - 動作処理情報テーブルを動的に生成することが可能
  - 一般の通信にほとんど影響を与えない
- 今後の課題
  - FPNをDPRP，IPsec/IKEで構築して管理負荷を評価
    - 初期設定
    - ネットワーク構成が変化した際に発生する設定変更

Performance evaluation of Dynamic Process Resolution Protocol

動作処理情報テーブル

- ハッシュテーブルとして実装



送信元		宛先		プロトコル	処理内容	グループ鍵情報	
IP	Port	IP	Port			番号	バージョン

- “Encrypt/Decrypt”
- “Transparent”
- “Discard”

DPRPの実装

- IP層に実装（入出力関数からcall）