自宅からのリモートアクセスを可能にする GSRAv2の提案と評価

103430015 鈴木 健太
渡邊研究室

1. はじめに

モバイル端末の小型・高性能化や，モバイルブロードバンドの普及に伴って，リモートアクセスのニーズが高まっている．リモートアクセスを実現する既存の技術には，IPsec-VPN，SSL-VPN，OpenVPN，PacketiX VPN などがある．これらの技術は設定が煩雑であったり，アドレス管理が必要になる等の方式的な課題がある．また，アクセスを行う端末がグローバルアドレスを持つことを前提としている場合が多い．IPv4 アドレスの枯渇を目前に控えた今，実際には，アクセスを行う端末はホームネットワークなどの NAT 配下に存在し，プライベートアドレスを保持している場合がほとんどである．我々は，セキュアなリモートアクセス方式として，GSRA（Group-based Secure Remote Access）[1, 2] を提案しているが，NAT 配下からは使用できないという課題があった．

そこで本論文では，GSRA を改良し，いかなる NAT 配下からでもリモートアクセスを可能にした GSRAv2 を提案する．GSRAv2 の実装を行い，既存方式と比較評価を行い，GSRAv2 の有用性を確認した．

2. GSRA とその課題

2.1 GSRA

GSRA は，NAT 越え技術 NAT-f（NAT-free Protocol）[3] にセキュリティ面の機能を追加することにより安全なリモートアクセスを実現した技術である．通信グループの概念を用いることにより簡単かつ柔軟なアクセス制御を行うことができる．アクセスを行う外部端末（EN）及び GSRA の機能を持ったアクセス先 LAN のルータ（GSRA ルータ）に予めアドレス変換テーブルを生成し，テーブルのエントリに従ってアドレス変換をしながらパケットを転送することにより，内部端末（IN）へのリモートアクセスを実現する．GSRA によるリモートアクセス開始時に行うネゴシエーションの流れを図 1 に示す．以下に各処理について述べる．

(1) 名前解決　EN は IN の名前解決を行い，GSRA ルータの G_{GR} を取得する．ここで EN はカーネル領域において，DNS 応答に記載されている IP アドレス G_{GR} を仮想 IP アドレス V_{IN} に書き換えてアプリケーションに通知する．これにより EN は IN の IP アドレスを V_{IN} と認識する．

(2) トリガパケットの送信　EN から V_{IN} 宛のパケットがはじめて送信される時，このパケットを待避し，以降の (3)，(4) の処理を行う．

(3) グループ認証処理　EN は IN のホスト名 “Alice” と自身のグループ情報 “Group1” を記載したグループ認証要求を GSRA ルータへ送信する．GSRA ルータはこれを受信すると，登録されているグループ情報から，アクセス認証を行う．アクセスが許可された場合，当該セッションに使用するポート番号 t を予約し，t を記載したグループ認証応答を EN へ送信する．EN はグループ認証応答メッセージから t を取得し，V_{IN} と，$G_{GR} : t$ を対応付けるための VAT（Virtual Address Translation table）を生成する．

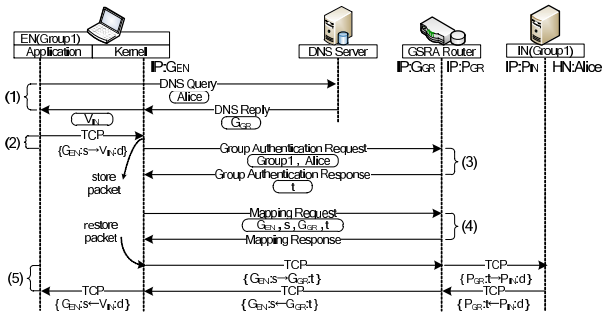


図 1: GSRA ネゴシエーションの流れ

(4) マッピング処理　EN は，自身の $G_{EN} : s$ と，(3) で取得した $G_{GR} : t$ を記載したマッピング要求を GSRA ルータへ送信する．GSRA ルータはマッピング要求メッセージから取得した情報を用いて，(3) で予約された $G_{GR} : t$ と，IN の $P_{IN} : d$ を対応付ける GSRA マッピングテーブルを生成する．続いて（2）で待避したパケットを復帰させ，通信を開始する．

(5) IN へのアクセス　復帰させた通信パケットは，まず EN の VAT に従い宛先 IP アドレス/ポート番号が変換され，GSRA ルータへ送信される．GSRA ルータでは，GSRA マッピングテーブルに基づいて宛先/送信元の IP アドレス/ポート番号を変換し，IN へと転送する．IN から EN への応答は上記と逆の順序でアドレス変換および暗号化処理を行い，EN まで届けられる．以降の通信パケットも同様に処理され，IN へのリモートアクセスが実現する．

2.2 GSRA の課題

GSRA では，EN 側の NAT（HR）によって送信元情報が変換されてしまうと，正しいマッピングテーブルが生成できないという課題があった．そのため，HR による変換内容を予め知っておく必要があるが，一般的な方法では，HR に搭載された SPI（Stateful Packet Inspection）機能によりネゴシエーション完了後の通信パケットが破棄されてしまう．従って，SPI 機能を搭載した HR の配下からでも通信を開始できるような手段が新たに必要となる．

3. 提案方式

上記の課題を解決するためのバインディング処理を新たに追加した GSRA を GSRAv2 と呼ぶ．バインディング処理では，HR による変換内容を予め取得するとともに，TCP の再送制御の特徴を利用することで SPI によるパケット破棄を回避している．図 2 に GSRAv2 のネゴシエーションの流れを示す．バインディング処理では，まず EN が ICMP による Binding Request（$BReq_i$）を GSRA ルータへ送信

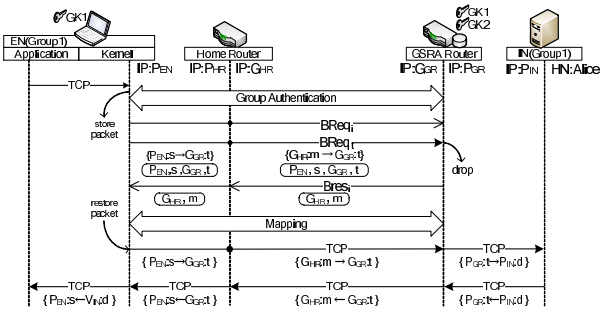


図 2: GSRAv2 ネゴシエーションの流れ

する．EN はこのパケットの応答を待たず，続けて TCP による Binding Request（$BReq_t$）を GSRA ルータへ送信する．$BReq_t$ は，トリガとなった TCP パケットを内容をコピーし，宛先を $G_{GR} : t$ に書き換えたものである．GSRA ルータは $BReq_i$ を受信すると，受信したパケットを待避する．続いて $BReq_t$ を受信すると，そのヘッダ情報から，HR による変換後の $G_{HR} : m$ を取得して，応答を返さずこのパケットを破棄する．その後，待避していた $BReq_i$ に対する Binding Response（$BRes_i$）を生成し，取得した $G_{HR} : m$ を記載して EN へ送信する．以上のバインディング処理により，GSRA ルータと EN は HR による変換内容を得ることができる．また，ネゴシエーション完了後に送信されるパケットは，応答を返さなかった $BReq_t$ の再送パケットとして HR に扱われることになる．TCP の再送パケットに見せかけることで，HR では再送前と同じポート番号が割り当てられるため，後のマッピング処理において，HR に対応したマッピングテーブルを生成することが可能となる．$BReq_t$ の中身は，トリガとなったパケットをコピーしていたため，HR を通過するパケットのシーケンス番号などの情報に整合性が保たれており，SPI によるパケット破棄を回避することができる．以上の方法により，GSRAv2 はいかなる NAT 配下からでもリモートアクセスが可能となる．

4. 比較評価

既存方式と提案方式で，機能面及び性能面の比較評価を行った．

4.1 機能面の評価

表 1 に，機能面の比較を示す．GSRAv2 は，EN に専用ソフトをインストールする必要があり，現在は FreeBSD にしか対応していない．しかし，エンドエンドで暗号化通信が可能，高スループット，アプリケーションの制約が無い，アドレス管理を必要としないなど，既存方式に比べ機能的に優れていると言える．

4.2 性能面の比較

FreeBSD に実装したの提案方式を用いて，通信開始時に発生するオーバヘッド時間及び，スループットを測定し，性能を評価した．比較対象は，IPsec-VPN と OpenVPN，PacketiX VPN の 3 手法である．

- **通信開始時のオーバヘッド時間**

  表 2 に通信開始時に発生するオーバヘッド時間の測定結果を示す．IPsec-VPN，OpenVPN は，約 3s，PacketiX VPN は，約 200ms のオーバヘッドが発生するが，GSRAv2 は，約 60ms で通信を開始できた．以上の結果から，GSRAv2 は最も短時間でリモートアクセスを開始できることが確認できた．

表 1: 既存方式との比較

	IPsec-VPN	OpenVPN	PacketiX	GSRAv2
E2E 暗号化	×	×	×	○
スループット	×	△	×	○
HR 対応	△	△	△	○
クライアントソフト	△	×	×	×
アプリケーション	○	○	○	○
アドレス管理	×	×	×	○

表 2: ネゴシエーション時間の測定結果

	オーバヘッド時間 [ms]
IPsec-VPN	2924
OpenVPN	2574
PacketiX VPN	224
GSRAv2	61

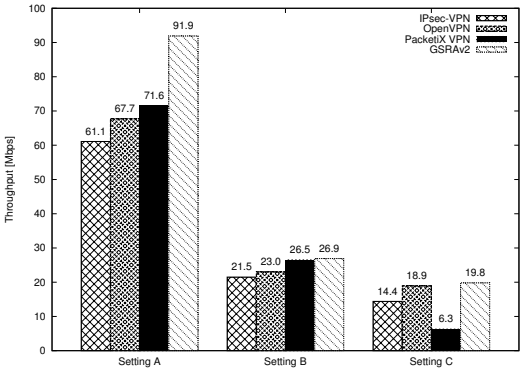


図 3: スループット測定結果

- **スループット**

  スループットの測定には，背景負荷として，A : 背景負荷なし，B : RTT20ms，C : RTT20ms かつパケットロス率 0.05%，の 3 パターンを設定した．図 3 に測定結果を示す．いずれの場合においても，GSRAv2 は最も高スループットを発揮できることが確認できた．既存の方式は，カプセル化によるヘッダオーバヘッドの増加，フラグメントの発生によりスループットが低下すると考えられる．一方，GSRAv2 は，カプセル化を必要としないため，スループット低下が起きない．

5. まとめ

本論文では，いかなる NAT 配下からでもリモートアクセスを可能にした GSRAv2 を提案し，既存方式との実機での性能比較を通じて，GSRAv2 の有用性を示した．今後は，Windows をはじめとした他の OS のへの実装を進め，普及を目指していく．

参考文献

[1] 鈴木秀和，渡邊　晃 : 通信グループに基づくサービスの制御が可能な NAT 越えシステムの提案，情報処理学会論文誌，Vol. 51, No. 9, pp. 1881–1891 (2010).

[2] 鈴木健太，鈴木秀和，渡邊　晃 : NAT 越え技術を応用したリモートアクセス方式の提案と設計，マルチメディア，分散，協調とモバイル（DICOMO2010）シンポジウム論文集，Vol. 2010,No. 1, pp. 288–294 (2010).

[3] 鈴木秀和，宇佐見庄五，渡邊　晃 : 外部動的マッピングにより NAT 越えを実現する NAT-f の提案と実装，情報処理学会論文誌，Vol. 48, No. 12, pp. 3949–3961 (2007).

自宅からのリモートアクセスを可能にする GSRAv2の提案と評価

名城大学大学院 理工学研究科
情報工学専攻　渡邊研究室

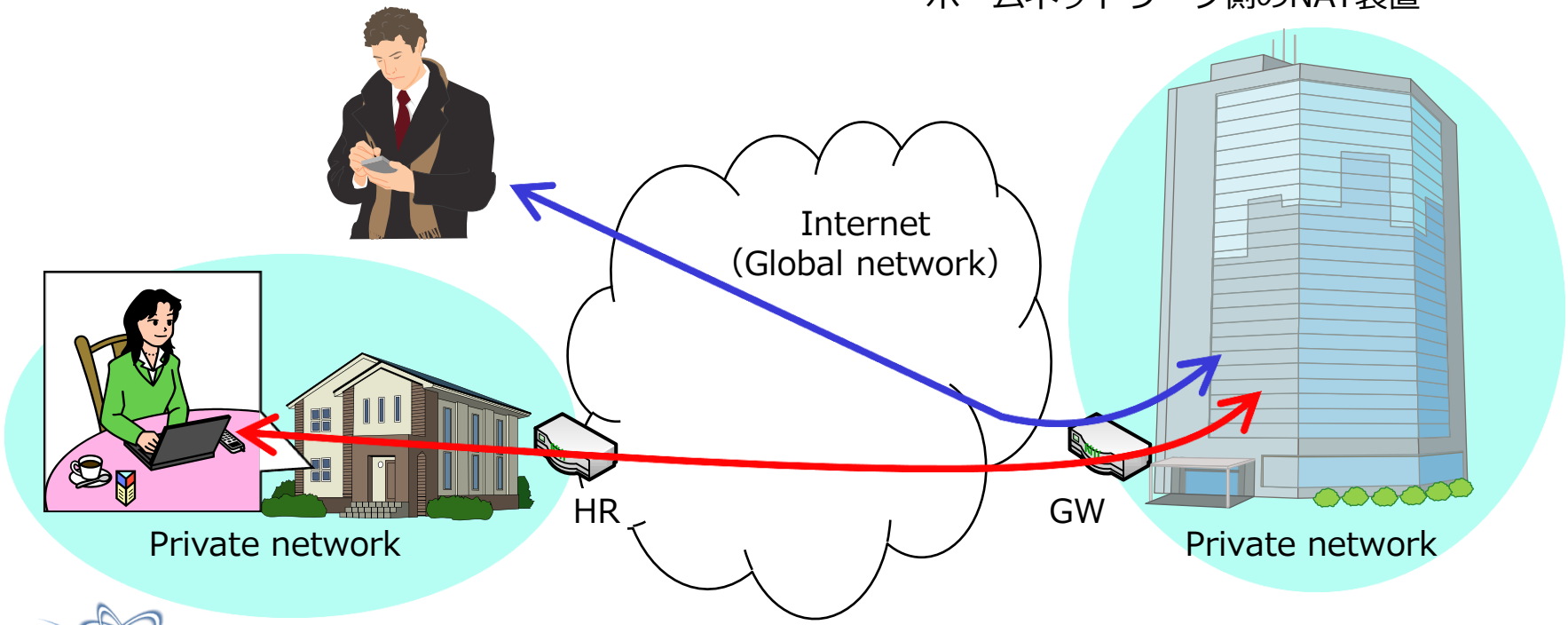
103430015　鈴木 健太

研究背景

- リモートアクセス需要の増加
  - 遠隔地のネットワークに接続
  - 利用形態の変化
    - これまで：出張先から社内LANへアクセス：Global → Private
    - 近年：自宅から在宅勤務や学内サイト閲覧：Private → Private

➔HR※配下からの利用

※HR(Home Router)
└ホームネットワーク側のNAT装置

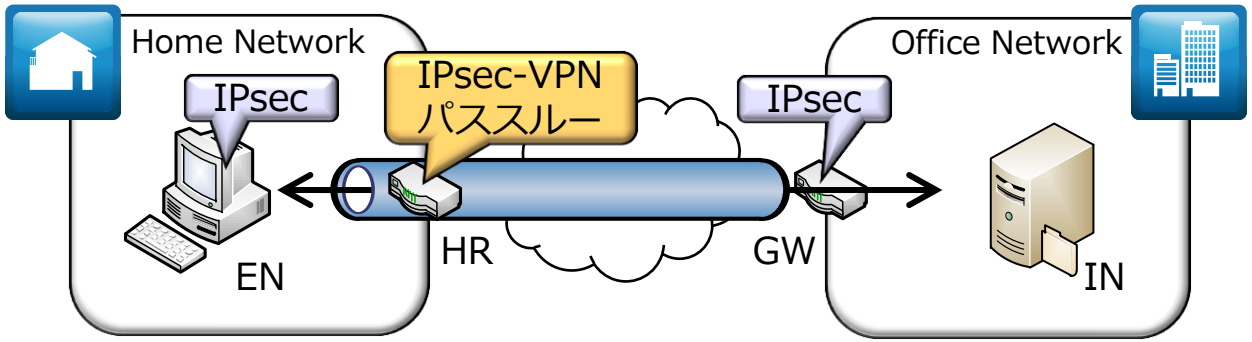


既存のリモートアクセス方式

- IPsec-VPN
- OpenVPN
- PacketiX VPN
- GSRA

既存方式：IPsec-VPN

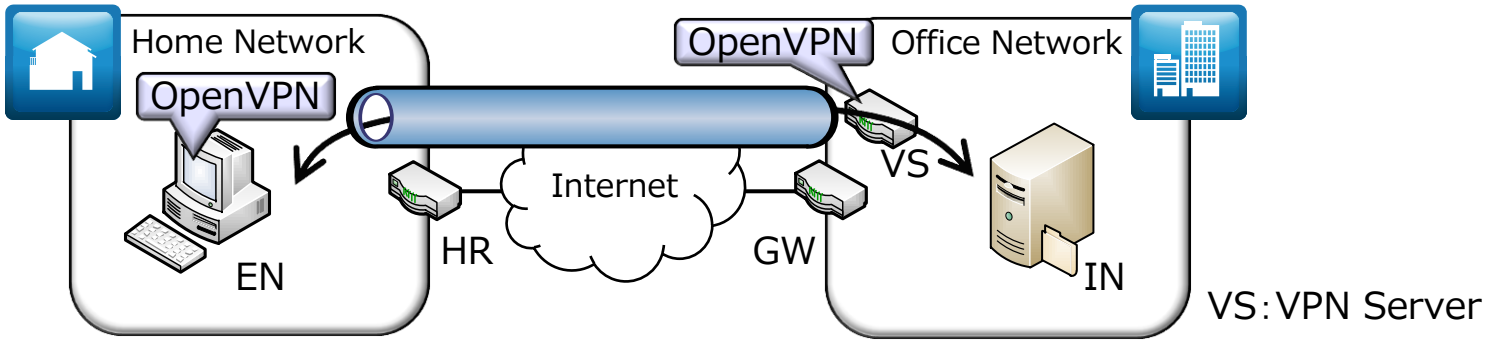
EN(External Node)：リモートアクセスを行う端末
IN(Internal Node) ：アクセス対象の端末



- IPsecの仕組みを利用してVPNを構築
  - 通信相手端末1台毎に設定が必要➔設定が煩雑
  - パケットをカプセル化➔通信性能低下
  - NATによるアドレス変換=偽装とみなして破棄
    - NAT traversal＋IPsecパススルーが必要
  - アドレス管理が必要
    - プライベートIPアドレスが重複しないよう管理する

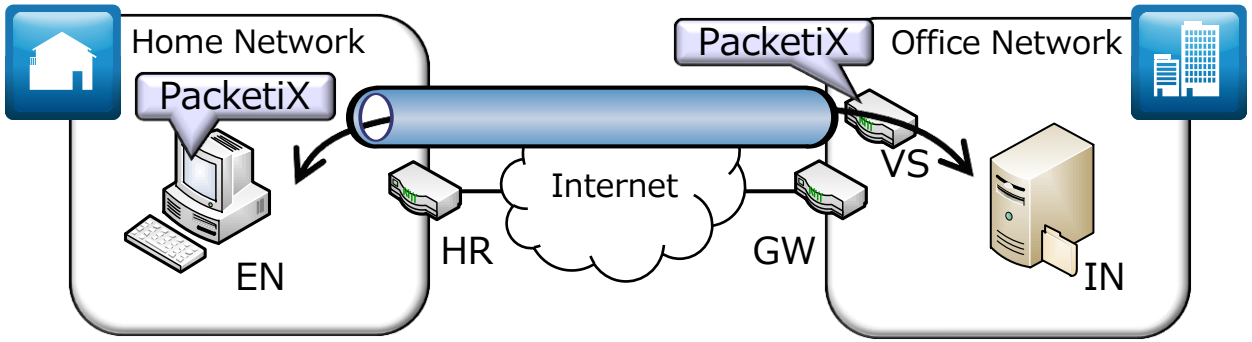
HRありの場合

既存方式：OpenVPN



- SSLを用いたオープンソースVPNソフトウェア
- 仮想インターフェース間でトンネリング
  - 多くのOSに対応,混在も可能
  - パケットをカプセル化➔通信性能低下
  - アドレス管理が必要 ）HRありの場合

既存方式：PacketiX VPN



- ソフトイーサ㈱が開発したVPNソフトウェア
- 独自の仮想インターフェース間でトンネリング
  - パケットをSSLに偽装
    - 管理者に知られぬままVPNトンネルを構築可能
      - ウィルス侵入，情報漏えいの危険性
  - TCPでカプセル化・・・TCP over TCPの問題
  - アドレス管理が必要 ）HRありの場合

既存方式：GSRA

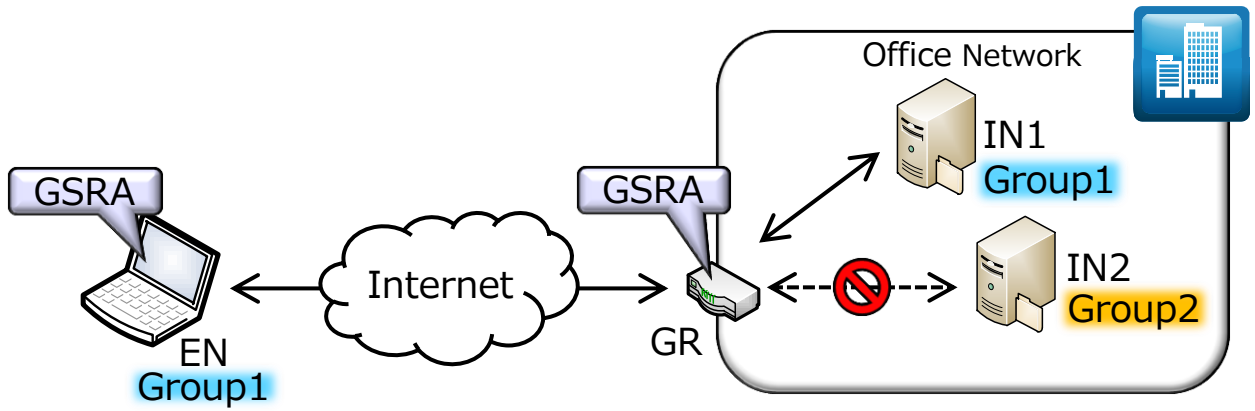
- GSRA（Group-based Secure Remote Access）

＝ NAT越え ＋ アクセス制御

- アドレス変換による中継通信
  →非カプセル化・高スループット
- グループの概念を利用
  →柔軟かつ簡単なアクセス制御

→ 既存方式の欠点を解決

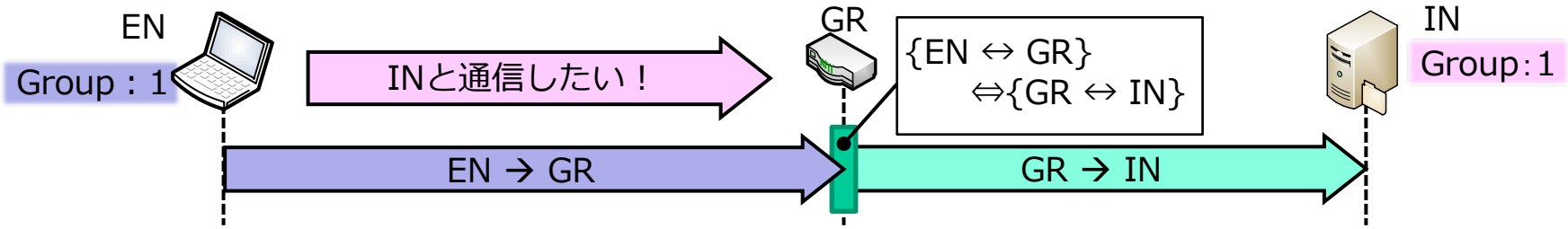
×HR配下から使用できない



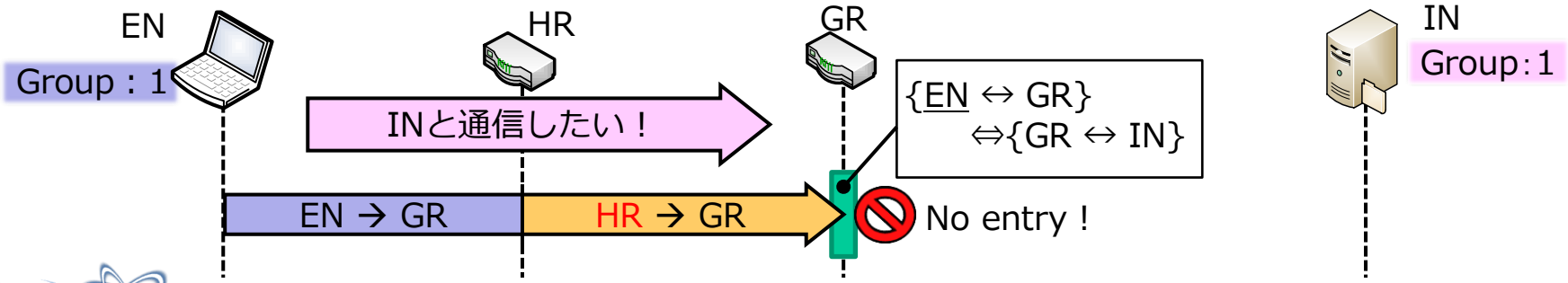
GR：GSRA Router

GSRAの仕組みと課題

- GSRAルータにアドレス変換テーブルを生成
  - ENとINの対応付け
  - アドレス変換によるリモートアクセス

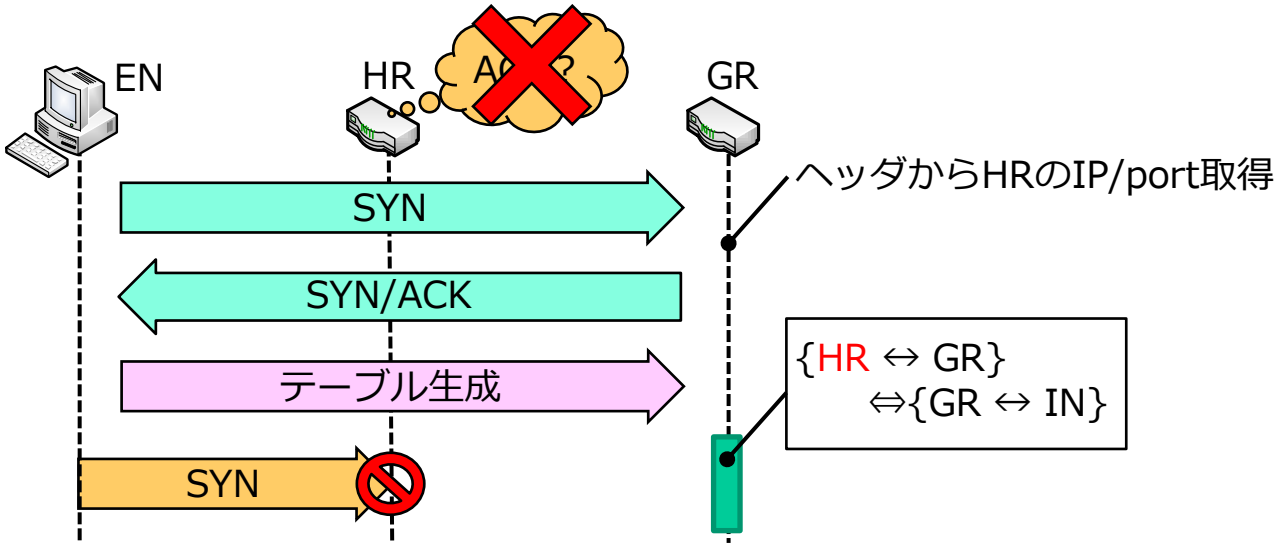


- HR配下から使用する場合
  - ヘッダ情報のみが変換される
  - 生成されるテーブルはHR無しの場合と同じ
    →該当するテーブルエントリが存在しないため通信できない



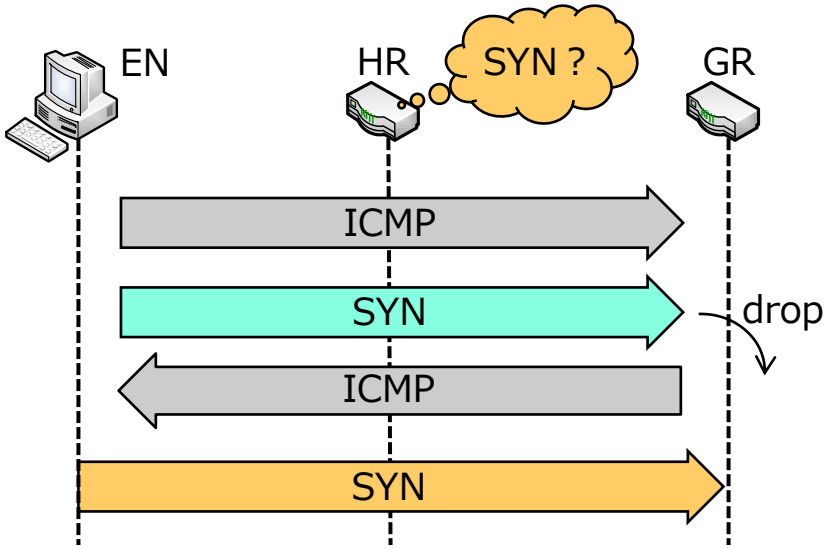
HR対応方法の検討

- TCP1往復のシーケンスを追加する
  - 予めHRで割り当てられるアドレス/ポート番号を得る
    →HRに対応したテーブルが生成可能
- 一方HRでは・・・
  - SYN，SYN/ACKの通過を記録
    - 次はACK
  - 実際に送信されるのはSYN
    - シーケンス不整合→破棄



解決策

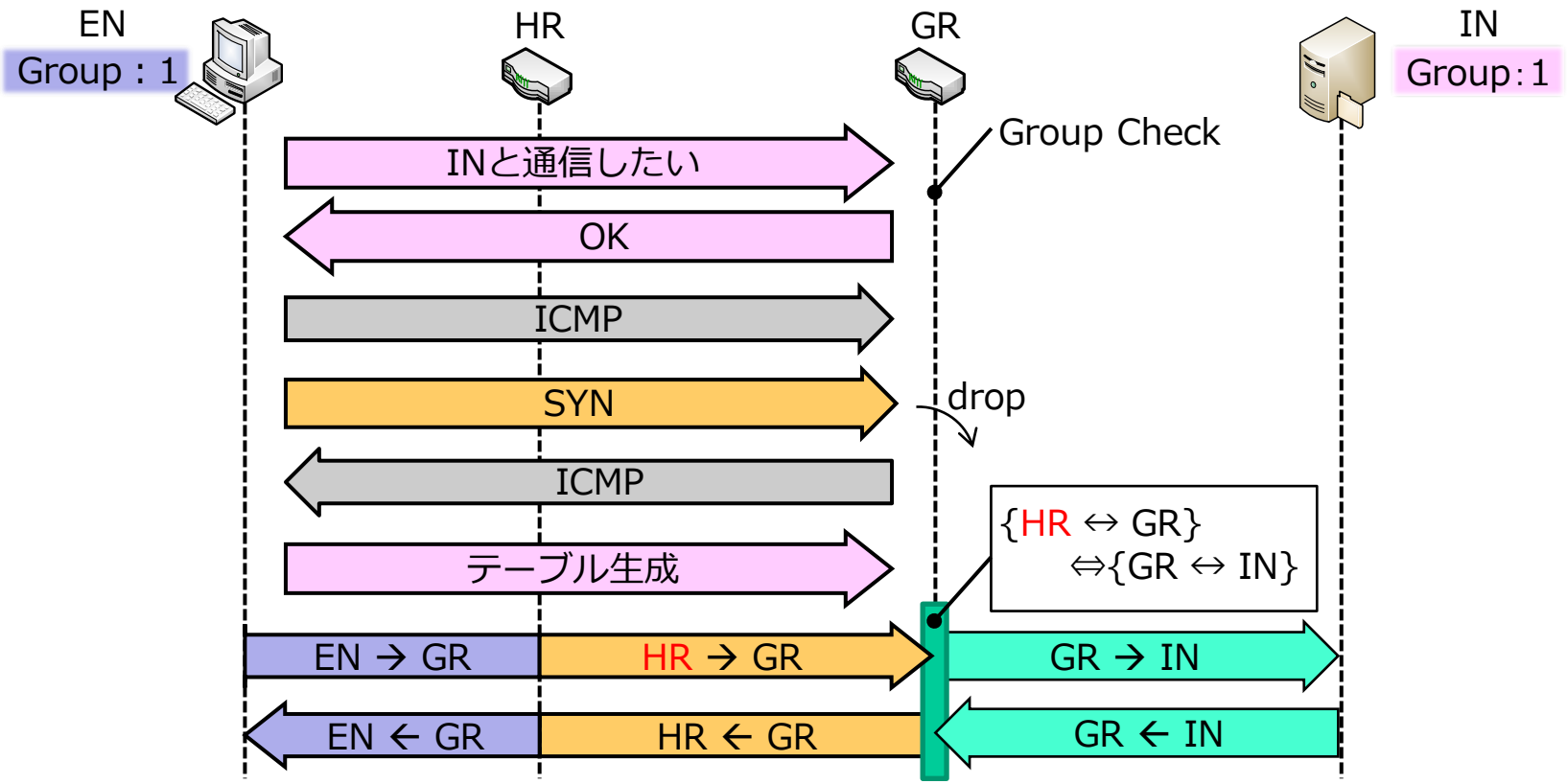
- テーブル生成後のSYN←不自然でない状態にすればよい
  - TCPの再送制御に着目
  - SYNのみ送信し，応答を返さず意図的に破棄
    - HRはSYNがロスしたと判断し，SYNの再送を待つ
  - ENへの通知はICMPで行う
    - 整合性に関わらず通過可能



この方法をGSRAに適用する

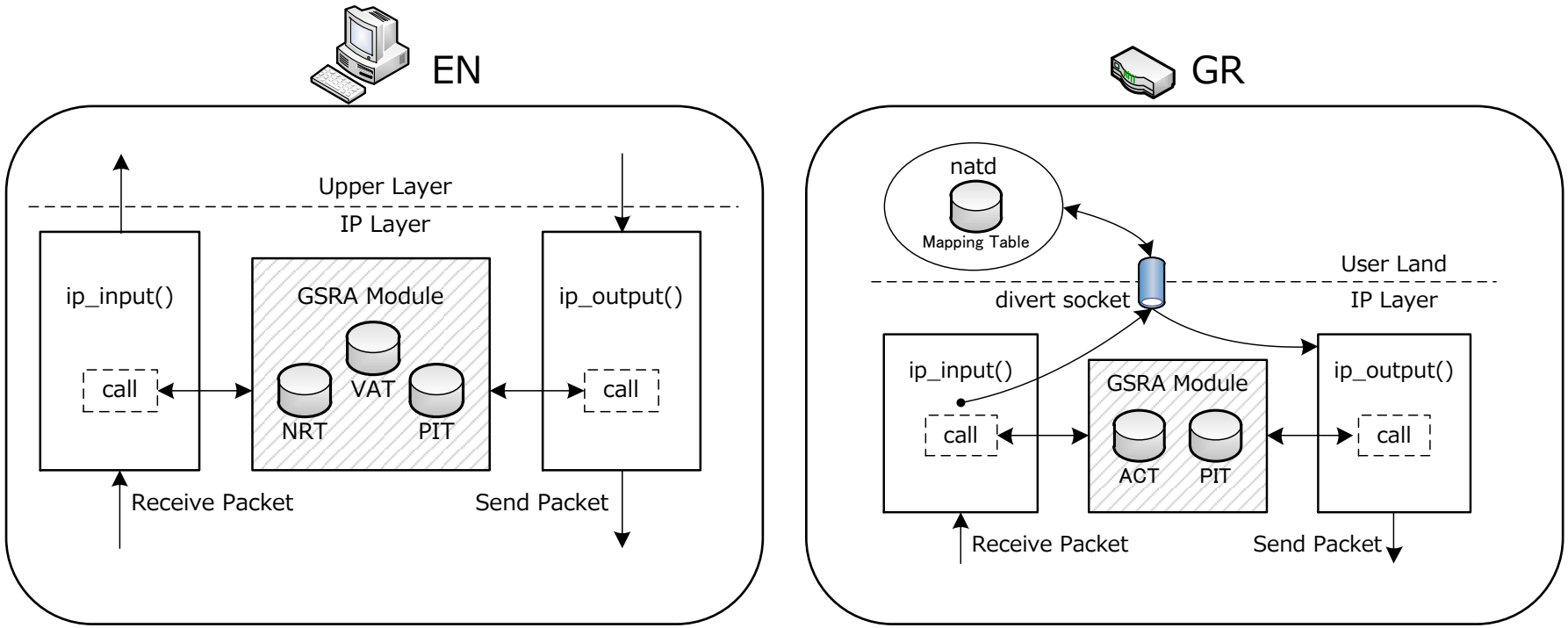
提案方式-GSRAv2

- 特殊な1.5往復シーケンスの追加によりHRに対応
- GSRAの特長をそのまま受け継ぐ



実装

- FreeBSDへ実装
  - パケットをIP層で横取り
  - GSRAモジュールでアドレス変換などの処理
    - 機能拡張，処理変更



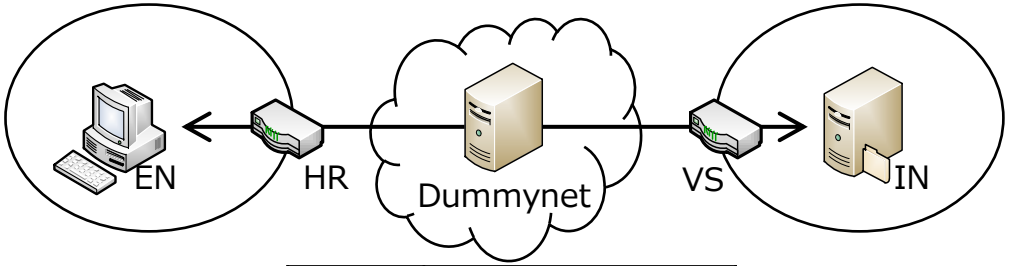
性能測定

- 測定項目
  - 通信開始時のオーバヘッド時間
  - スループット

- 比較対象
  - IPsec-VPN
  - OpenVPN
  - PacketiX VPN

測定環境

- インターネット越しの利用を想定
  - Dummynetにより背景負荷をかける
    - 実測に基づいた伝送遅延とパケットロス率



Delay	Packet Loss Rate
10 ms	0.05 %

	OS	CPU	Memory	NIC
External Node	FreeBSD 7.2※	Pentium4 3.4 GHz	1 GB	1000Base-T
Home Router	FreeBSD 7.2	Pentium4 3.0 GHz	512 MB	1000Base-T
Dummynet	FreeBSD 8.0	Pentium4 2.8 GHz	512 MB	1000Base-T
VPN Server	FreeBSD 7.2	Pentium4 3.4 GHz	2 GB	1000Base-T
Internal Node	FreeBSD 7.2	Pentium4 2.8 GHz	1 GB	1000Base-T

※PacketiX VPNのみWindows 7

性能測定（方法）

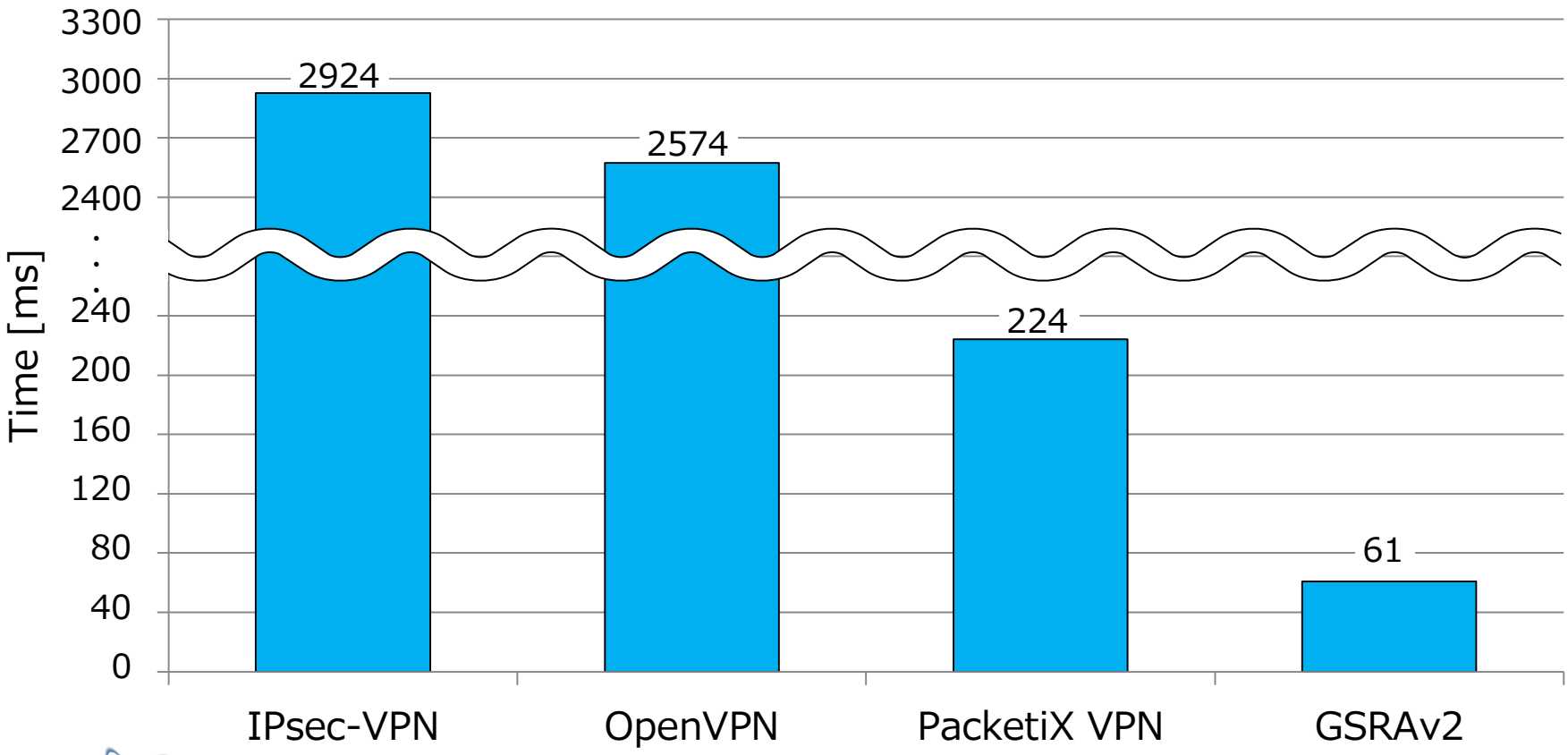
- 通信開始時のオーバヘッド時間
  - Wiresharkでネゴの様子をキャプチャ（EN）
  - 10回試行した平均値を測定値とする
  - 背景負荷あり

- スループット
  - wget※でINから1GBのファイルをダウンロード
  - wgetで算出されたスループットを採用
  - 10回試行した平均値を測定値とする
  - 背景負荷あり，なしともに測定

※http://www.gnu.org/software/wget/

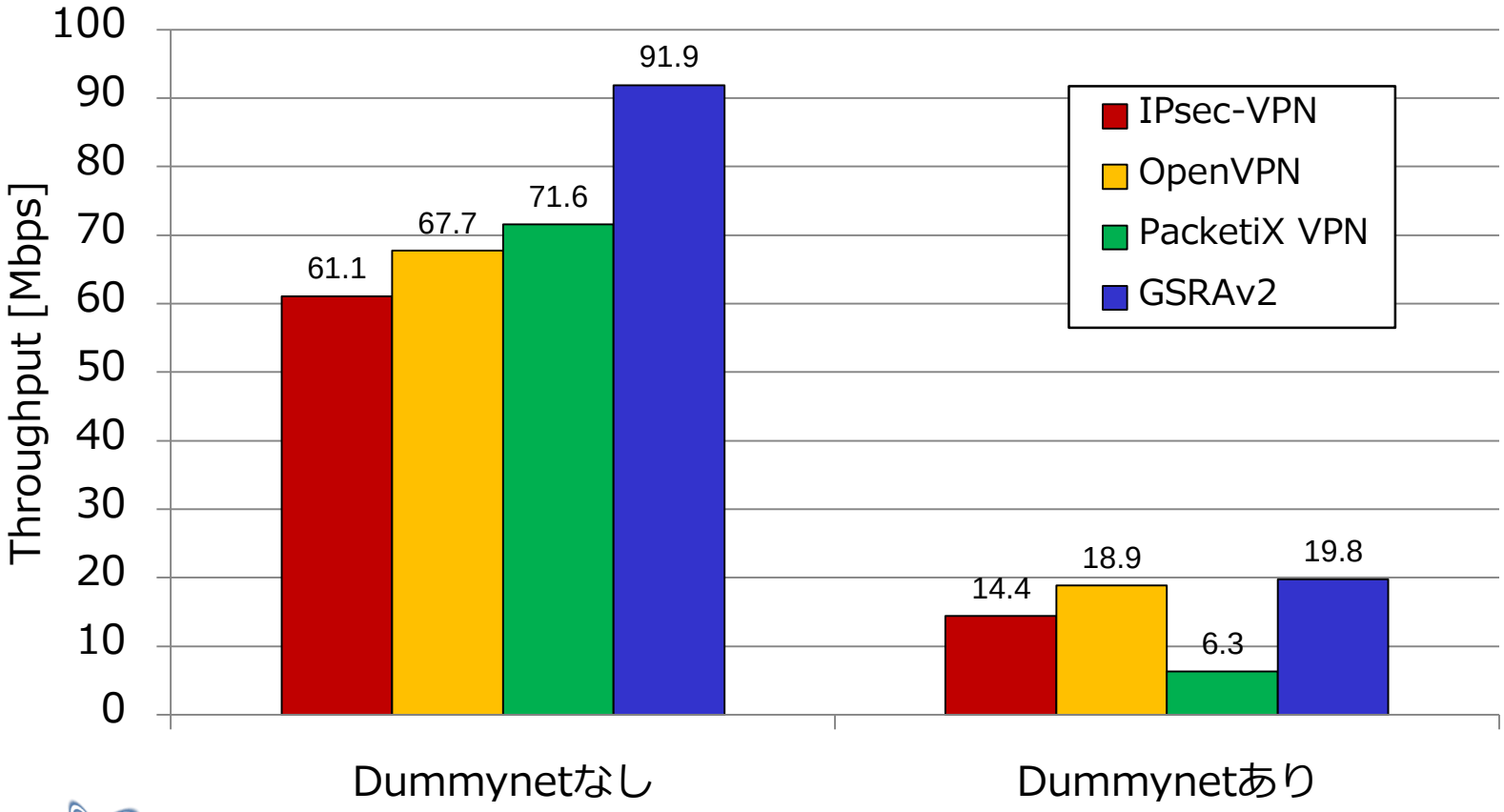
測定結果（通信開始時のオーバヘッド時間）

- GSRAv2は他方式の3分の1以下の時間で通信開始可能
  - ネゴシエーションシーケンスは3往復のみ
  - カーネル内で全て処理



測定結果（スループット）

- 条件に関わらずGSRAv2が最も高スループット
- PacketiX VPNのスループットが大幅に低下
  - パケットロスの発生によりTCP over TCP問題が顕在化



まとめ

- GSRAv2を提案した
  - GSRAの特長をそのまま受け継ぐ
  - HR配下から利用可能に
- 提案方式をFreeBSDに実装し，性能測定を通じて有用性を確認した
  - 短時間の処理でリモートアクセスを開始できる
  - 背景負荷に関わらず高スループット
- 今後の課題
  - 他OSへの対応

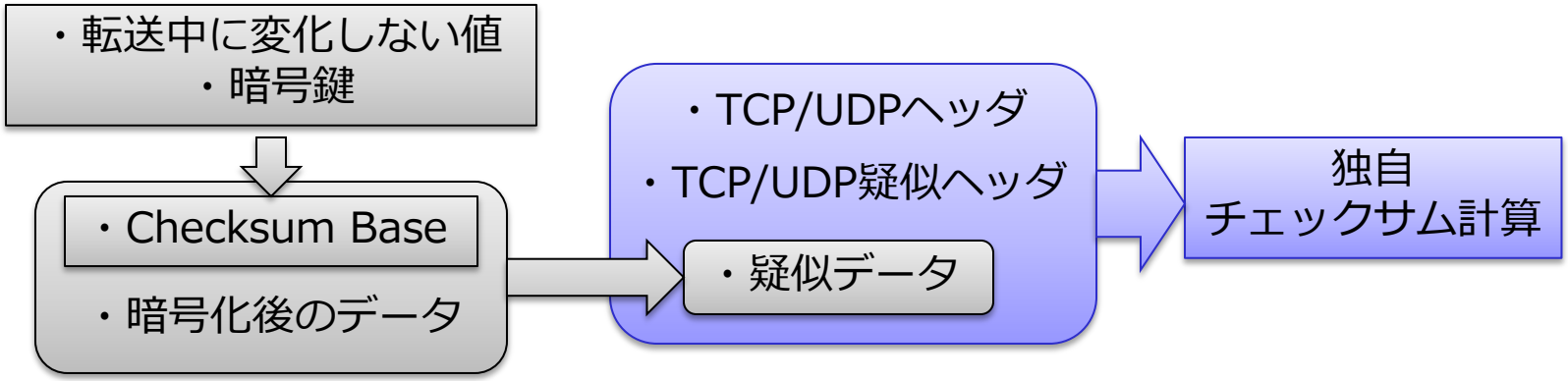
比較評価

- GSRA：既存方式の課題を解決
- HR配下からの利用も可能
- 性能評価により通信性能の高さも証明

	IPsec-VPN	SSL-VPN	OpenVPN	PacketiX VPN	GSRAv2
クライアントソフト導入の必要性	△	△	✕	✕	✕
エンドエンド暗号化	✕	△	✕	✕	△
アプリケーション制約	○	✕	○	○	○
カプセル化オーバヘッド	✕	△	✕	✕	○
アドレス管理必要性	✕	○	✕	✕	○
HR通過	△	○	○	○	○
通信開始時のオーバヘッド時間	△	ー	△	○	◎
スループット	○	ー	○	△	◎

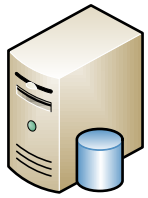
PCCOM

- 独自のTCP/UDPチェックサム計算
  - 本人性確認とパケットの完全性保証
- 暗号化範囲＝TCPペイロード部
  - NATをまたがった暗号通信が可能
- パケットフォーマットに変更を加えない
  - 高スループット



仮想アドレスの生成

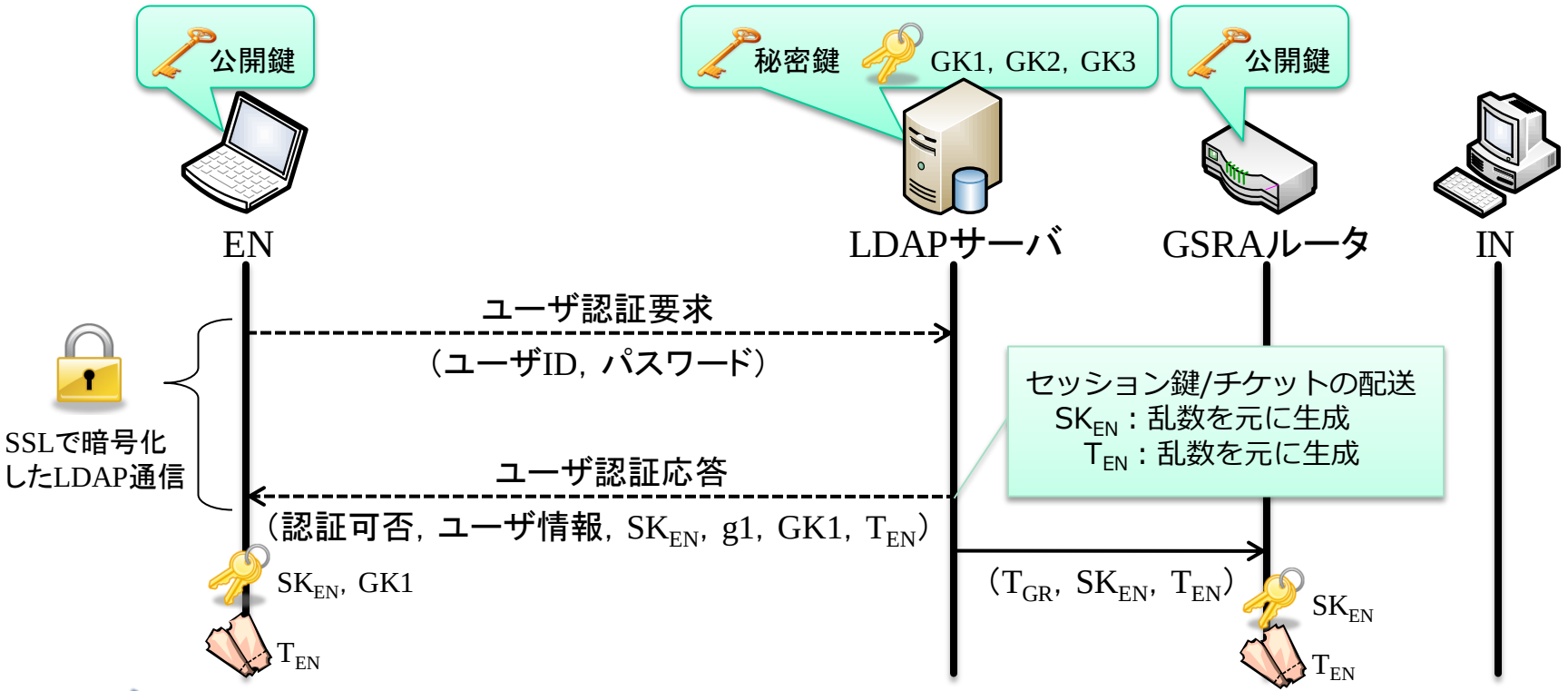
- INのFQDNから生成する
- V_{IN}＝A.B.C.D
  - A：仮想アドレスと認識するための値
    - ENから到達性がない値
  - B：初期値=0
    - 仮想アドレスが重複した場合に変化させる
  - C：ドメイン名(example.net)のハッシュ値
  - D：ホスト名(alice)のハッシュ値



IN：alice.example.net

グループ鍵の配送

- LDAP（Lightweight Directory Access Protocol）
  - ディレクトリサービスへアクセスするためのプロトコル
  - ユーザ名などのキー値から情報を検索することが可能



ENがPCCOMをサポートする場合

- INにPITを生成
- GSRAルータはアドレス変換のみ行う