本資料について

本資料は下記著書を基にして作成されたものです。
著書の内容は保障できないため、正確な知識を求める方は原本を参考にしてください。

- 文献名
  - IPsecover NAT Justification for UDP Encapsulation
- 分類
  - Internet-Draft

輪講発表

名城大学　理工学部　情報科学科
渡邊研究室
01J078　播磨宏和

IPsec over NAT Justification for UDP Encapsulation

UDPカプセル化のための IPsec over NAT 配置

Introduction

イントロダクション

Introduction

今日、インターネット接続を共有するために、NATが広く利用されている。

全てのルータやデバイスの標準機能として取り付けられている。

光ケーブル、DSLの発展により、様々な機器にNATを取り付けるということになりました。

例えば：ホテル、空港、公のワイヤレスサービス、
ISP（クライアントをインターネットに接続するためにNATを利用している）

Introduction（ NATとは）

NAT（Network Address Translation）とは、
インターネットに接続された企業などで、
一つのグローバルなIPアドレスを複数のコンピュータで共有する技術である。

組織内でのみ通用するIPアドレス(ローカルアドレス)と、
インターネット上のアドレス(グローバルアドレス)を透過的に相互変換することにより実現する。

最近不足がちなグローバルIPアドレスを節約できるが、
一部のアプリケーションソフトが正常に動作しなくなるなどの制約がある。

Introduction（ IPsecとは）

IPsec(IP Security Protocol)とは、

IETF（Internet Engineering Task Fors）が標準化を進めている、IPトラフィックを安全に保つための技術。

認証ヘッダ（AH）、IPカプセル化（ESP）、鍵の交換と管理方式（IKE）などの技術。

Introduction（問題）

L2TP/Ipsecにおいて、クライアントはNATを使ったインターネット接続をしている家に接続できない。

IPsecトランスポートモードによって保護されるTCP、UDPトラフィックは、ピアツーピア、サーバツーサーバ間のアプリケーションで交換されることができない。

Introduction（現状）

ベンダー製品は様々な方法で強制的にサポートする形となっている。

Introduction
（存在するNATを通過するために）

- UDPパケットのポートとアドレスを変換をする。
- 単純アドレス変換。

Introduction
（トンネルモードの通過）

NATをIPsecトンネルモードで通過するように許可させる。
アドレス割り当てにはIPsecメソッド上のDHCP標準トラックを使用。

しかし、IPsecトンネルの中のパケットによって使われた内部アドレスは、NATによって変換できない。

内部のIPパケットは目的ネットワーク上の無効なアドレスを保持してしまう。

Introduction
（トンネルモードの通過での解決）

トンネルの中のトラフィックがクリアテキスト
　TCP&UDPトラフィックである場合

IPsecトンネルの中のトラフィックが、IPsecトラン
　スポートトラフィックである場合

内部アドレスを使用して、目的地ネットワークを構
　成

heading as appropriate

heading as appropriate

NAT解決に関するIPsecのための必要条件

1.発展性
2.テレコミュータシナリオ
3.計測
4.サポートモード
5.総合運用
6.セキュリティ

Desgin Overview and Rationale

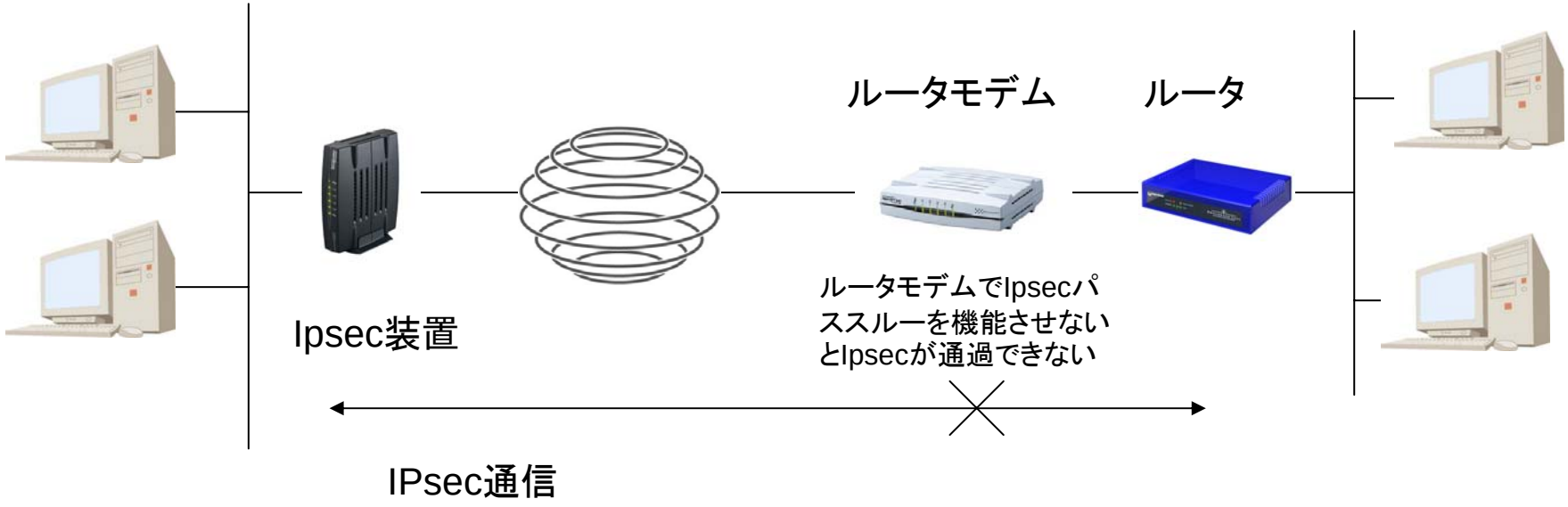
Desgin Overview and Rationale

- UDPポート500を使用するカプセル化
  - ファイヤーウォールルールを変更する必要が無い
- トラフィックプロテクションモードが最も効率的
- UDPポート500を使用するカプセル化は異なるポートを使用
- カプセル化より8バイト大きな個々のパケットを作る

IPSec NAT Traversal

IPSec NAT Traversal

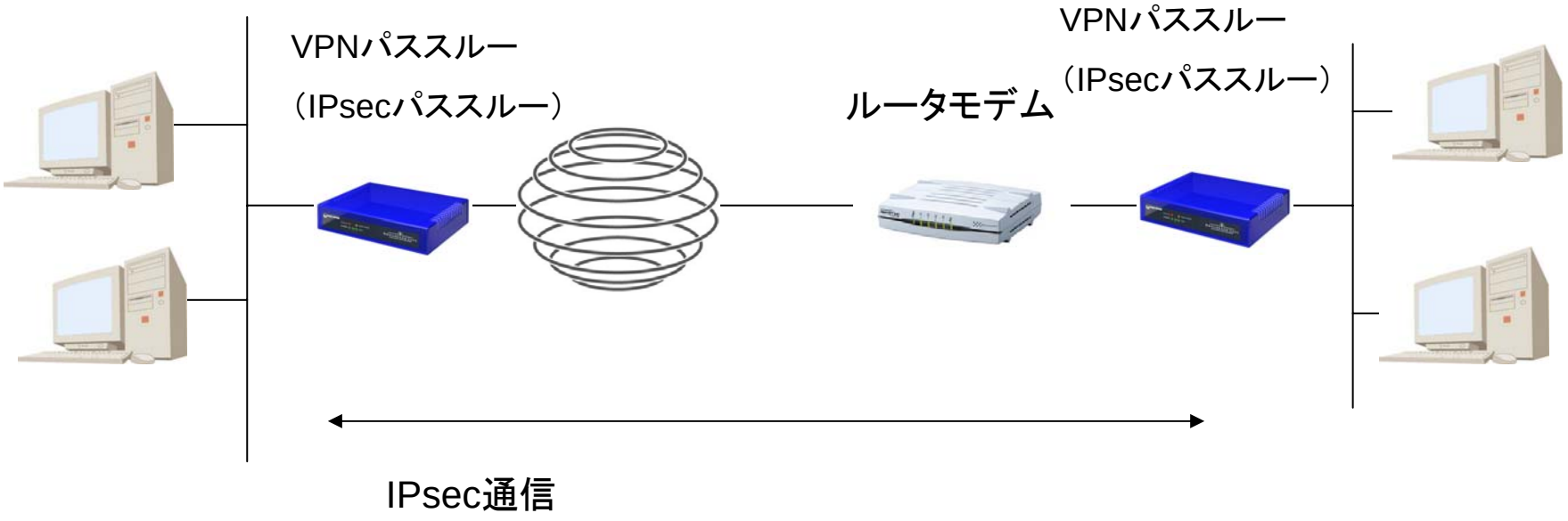
ルータタイプADSL回線でインターネットVPNを構築する場合、ルータモデムでIPsecパススルーを機能させる必要がある。



IPsecが経路上のIPマスカレードをこえて通信できないプロトコル上の問題が原因で、IPsec通信できないことがある。

この問題を解決するのが、NAT-Traversal機能。

NAT-Traversal機能は、IPsecパケットをUDPでカプセル化することで、この問題を解決し、IPsec通信を実現する。



UDP encapsulated ESP Header Format

UDP encapsulated ESP Header Format

偽造TCPとTCPヘッダーのオーバーヘッド
カプセル化のための好ましい選択としてUDPを選んだ。

- UDPヘッダは最小の標準カプセル化を8バイト提供。
- TCPヘッダは最小の20バイトを招くことになる。
- TCP接続を使用することは、スプーフされたTCPパケットによるリセット攻撃をうける。

UDP encapsulated ESP Header Format

NATポートマッピングが正確に保存されていることを保障

- IKE制御トラフィックおよびESPデータトラフィックの両方をカプセルに入れる。
- 既知のIKE UDPポート500を使用する。

Keep-alive Mechanism

Keep-aliveメカニズム

Keep-alive Mechanism

- Keep-aliveパケット
- IPsecピア間
- UDPパスを保持するために使用
- Keep-aliveパケットはパス・メンテナンスのために使用される。
- パケットは1や2ではなく、正常なTTL値で送られる。

終わり