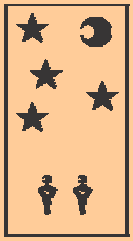
Internet Week 2001

IPsecによるVPN構築　第二部

IPsecによるVPNの設計ポイント

2001/12/6



株式会社ディアイティ
技術部
山田　英史

dit

1. 導入前

製品の“機能”と“性能”を見極める

- 機能面と性能面を評価し、ニーズに合った製品を選択。
  - 機能面
    - IPsecの実装レベル
    - 拡張機能
  - 性能面
    - スループット
    - SA数

IPsec機器の形態

- 製品形態による特性も考慮。
  - IPsec専用装置
    - 高スループット、低い故障率
    - *単機能*
  - IPsec機能付きファイアウォール
    - 機能の統合、アクセス制限
    - *煩雑な管理、障害切り分けの難しさ*
  - IPsec機能付きルータ
    - 機能の統合、低い故障率
    - *低スループット、機器自身のセキュリティ*
  - IPsec clientソフト
    - モバイル環境、低価格
    - *低スループット、分散管理*

目的やニーズの明確化

- 対象になるサービスは何か？
- 対象のホスト、セグメントは？
- 役割は？
- 規模は？
- ネットワークの種類は？
- 要求されるサービスの品質は？
- 利用者は？

既存ネットワークへの影響度を吟味

- IPsec-VPNを導入するネットワークを図に起こし、IPsec機器の設置箇所を吟味。特に既存のネットワークへの影響やサービスへの影響を考慮する。
- 現行のIPsecは、ほとんどの場合既存のネットワークに影響を与える。
- IPsec導入にあたって既存のネットワークの設定変更や組み換えが伴うことを覚悟する必要あり。

2. IPsec-VPN設計のポイント

ポイント

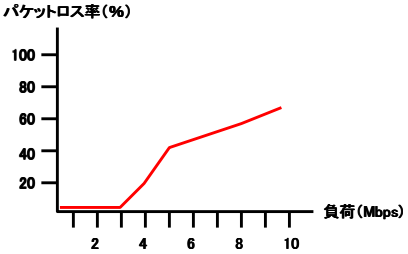
1. ネットワークインタフェースの種類
2. スループット・パフォーマンスに関する注意点
3. SAに関する注意点
4. 経路上のルータの設定
5. 分割されるネットワーク
6. IPアドレスの重複の回避
7. 平文通信許可時の注意点
8. フラグメンテーション
9. 認証方法の選択
10. NAT併用の注意点
11. Firewall併用時の注意点
12. その他ソリューションとの併用の注意点
13. IPsec clientの仕様
14. 管理機能
15. 障害対応
16. 輸出規制に関する注意点
17. 保守体制

1. ネットワークインタフェースの種類

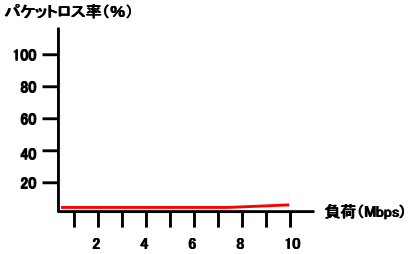
- 製品のネットワークI/F。
  - LAN
    - 10Base-T、100Base-TX
    - 半二重、全二重
  - リモート
    - BRI、シリアル
    - PPP、PPPoE

2. パフォーマンス・スループットに関する注意点

- ショートパケットが頻発するコンテンツ（音声や動画）を対象にする場合は、実測によるスループットの確認が望ましい。



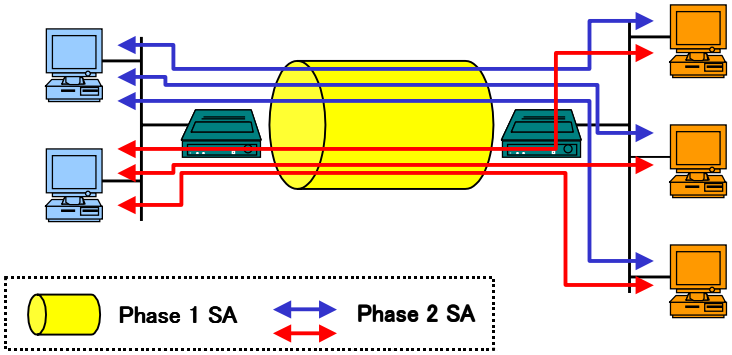
64byte長パケット送出
（カタログスペック10Mbpsの製品）



1440byte長パケット送出
（カタログスペック10Mbpsの製品）

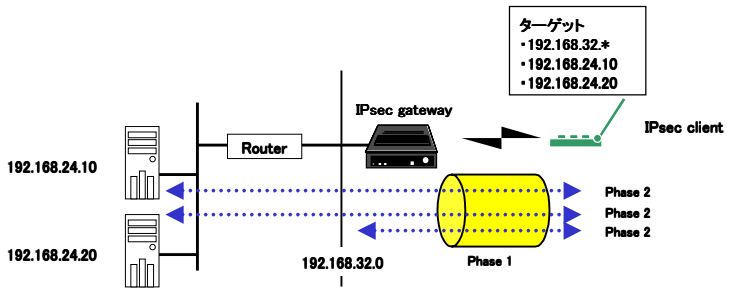
3. SAに関する注意点

- SA最大値
  - Phase 2はターゲット毎に確立
  - カタログスペックは曖昧
    - 実測が望ましいがPhase 1の試験は実現困難。



3. SAに関する注意点

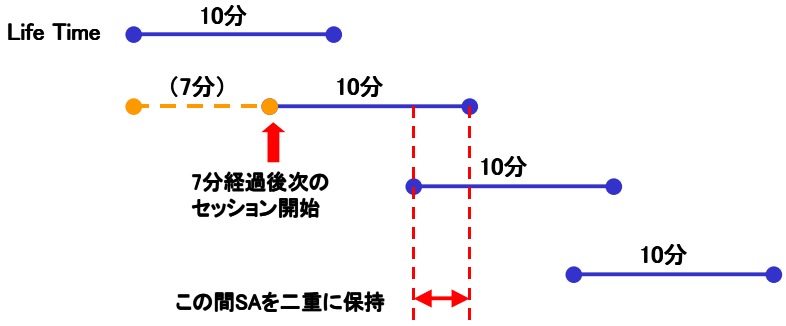
- SA数の予測



- 上図の例では1クライアント当たり4本のSAが確立している。
- ターゲットをホスト指定にするかサブネット指定にするかにより構築できるVPNの規模が変わる。

3. SAに関する注意点

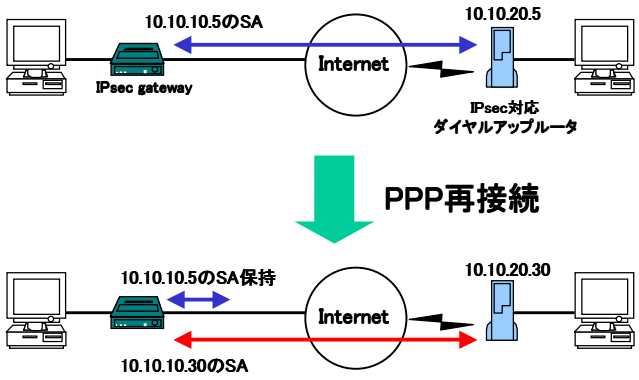
- Re-Key時のSA二重保持
  - 例えばフェーズ 2のLife Timeを10分と設定。
    - LifeTimeの何%で次のSAが準備されるかは製品によって異なる。
    - LifeTimeは経過時間以外にパケット数で設定できる製品も有り。



※フェーズ1はLife Timeの時点でいきなりRe-Key

3. SAに関する注意点

- リモートアクセス時のSA二重保持



3. SAに関する注意点

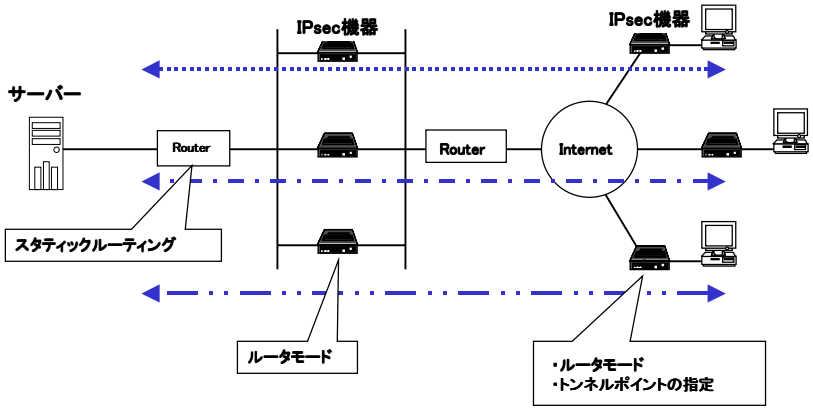
- 前述のような理由からPhase2 SAの数はカタログスペックの50%程度に考えた方が無難。
- 設備の問題でPhase1 SAの実装確認試験は難しい。今後の課題。

3. SAに関する注意点

- Re-Keyに要する時間
  - もし1ppsに1つSAが確立するとした場合、1000SAを張り終わるまで1000秒（約17分）必要になる。
  - 実際には高トラフィック（1ppsより速く）になるため、処理ロジックによってはさらに時間がかかる。

3. SAに関する注意点

- SAの分散。



4. 経路上のルータの設定

- IPsecでは様々なプロトコルを使用する。それらが透過的に流れるように経路上のルータのフィルタリングを設定。
- 特にISPのルータには注意。事前に申し入れることを推奨。

（1）IPsecで使用するプロトコル
UDP　　500　　ISAKMP
IP type 51　　AH (Authentication Header)
IP type 50　　ESP (Encapsulation Security Payload)

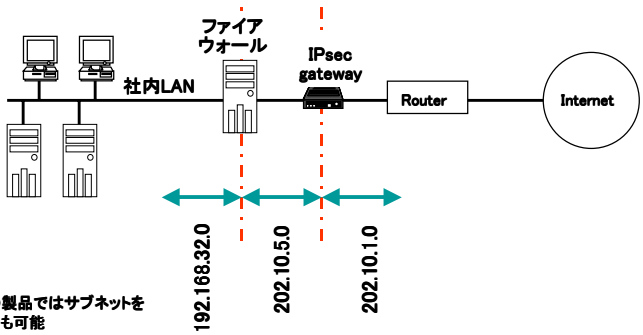
（2）ディレクトリサービスで使用するプロトコル
TCP 389（例）　LDAP

（3）CAが使用するプロトコル（Entrstの場合のデフォルト値）
TCP 709（例）　PKIX (Public Key Infrastructure X.509)
TCP 710（例）　Entrust administratorサービス

（4）その他、製品固有の管理用プロトコルなど
SSL, SNMP, FTP, 独自

5. 分割されるネットワーク

- トンネルモード（ルータモードという場合もある）で使用の場合、IPsec機器の前後でネットワークが異なる。
  - サブネットの再設定もありえる。



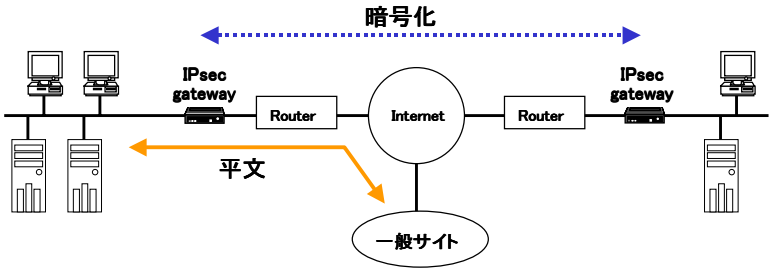
ブリッジモードサポートの製品ではサブネットを変更せずに設計することも可能

6. IPアドレスの重複の回避

- BtoBなどエクストラネットで他社拠点と接続する場合は、双方のプライベートアドレスの重複を避ける。
  - グローバルアドレスを割り振る。
  - NATによりグローバルアドレスに変換。

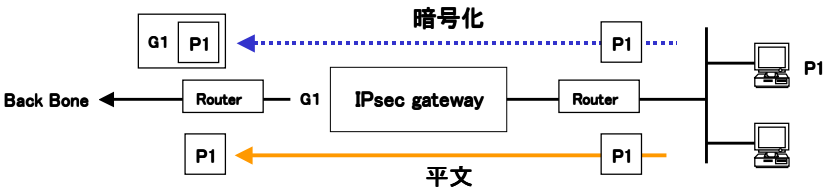
7. 平文通信許可時の注意点

- NAT機能やルーティングを持たない製品では、平文通過許可時の特性を確認する必要有り。



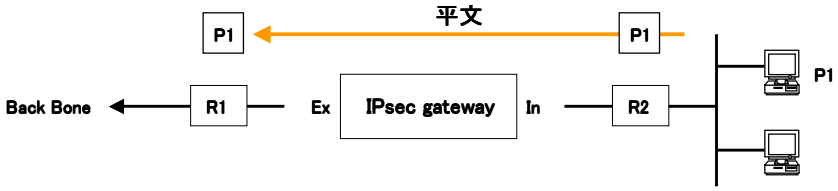
7. 平文通信許可時の注意点

- 平文通信を許すことで、認証によるアクセス制限はできなくなる。
  - バックボーン側からの平文の通過を許すことになる。もしセキュリティ上好ましく無い場合はファイアウォールやルータで不正アクセスを防ぐ。
- IPsec gatewayの内側のアドレスのままパケットが外に出ていく。
  - 暗号化される場合はパケットのアドレス(P1)はIPsec gatewayの外側のアドレス(G1)にカプセルされるが、平文のパケットは元のアドレス(P1)のままIPsec gatewayを通過する。
  - プライベートアドレスのままではインターネットにアクセス不可。



7. 平文通信許可時の注意点

- ルーティング
  - 製品によってはルーティングを行わないので、その場合はバックボーン側のルータ(R1)に「P1はEx ポートの後に存在する」というスタティクなルーティング情報を登録する。



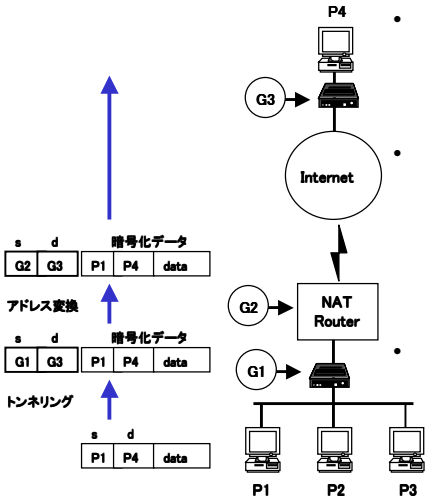
8. フラグメンテーション

- IPsecヘッダが不可されることで約40byte以上パケット長が延長される。フラグメンテーションが起きた場合の特性は製品によって異なる。
- 特に異機種間接続では実装の違いから通信不可になる場合がある。

9. 認証方法の選択

- IPsec標準のPre-Shared Key
  - 小規模VPNおよび1対n接続に向く。
- 拡張認証
  - RADIUS認証
    - モバイルVPNに適する。
    - IPsecではドラフト段階のため製品によりサポート状況に差あり。
    - 各種認証デバイス(ワンタイムパスワード等)による認証強化が可能。
  - CA認証
    - モバイルVPNおよび大規模VPN(n対n接続)に適する。
    - IPsecではドラフト段階のため製品によりサポート状況に差あり。
    - 各種認証デバイス(ICカード等)による認証強化が可能。

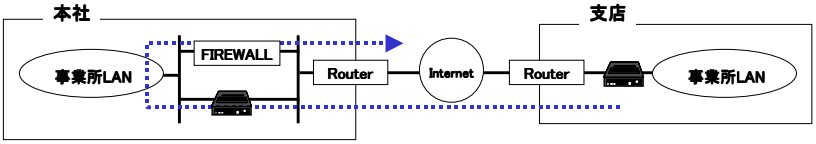
10. NAT併用の注意点



- NATによるアドレスの付け替えはIPsecとしては「なりすまし」として認識される(AH使用の場合)。
- IPsecではTCP/UDPも暗号化するので、ポート番号等が見えなくなる。IPますカレード等では、NATルータが複数のセッションを管理するための情報がなくなることになる。
- ESPではスタティックNAT(静的なアドレス変換)であれば可能。

10. NAT併用時の注意

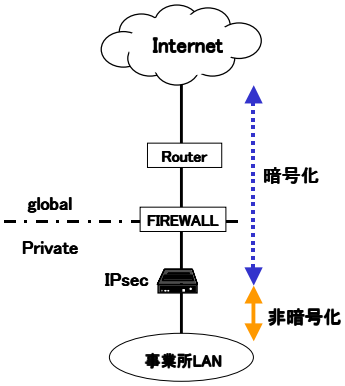
- NAT併用時問題点の回避策
  - NATルータ自身がIPsecを実装。
  - NATを使用しない。
    - 端末にグローバルアドレスを割り振る。
    - 下図のように小規模拠点は(支店)暗号化通信のみ行い、一般のInternetサービスへアクセスする場合は本社を経由する。
  - NAT Traversalの標準化により問題解決。



11. Firewall併用時の注意点

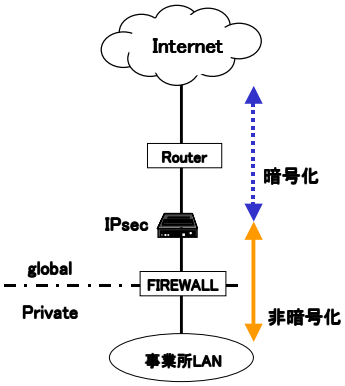
- ポート番号などの情報が欠けるため、暗号化されたデータはFirewallを通過出来ない場合がある。
- FirewallがNATをする場合の問題もある。

11. Firewall併用時の注意点



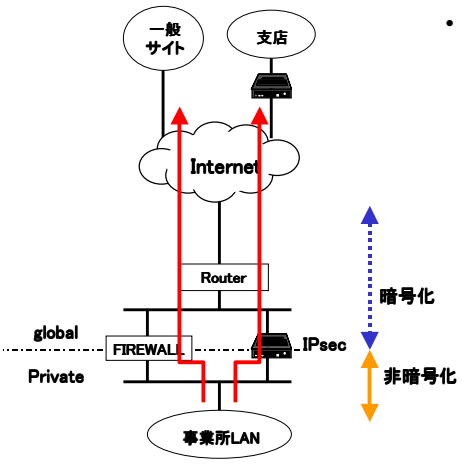
- Firewallの内側へIPsecを置く場合
  - 暗号化パケットを通過させるために様々な設定をFirewallに行う必要が有る。
  - FirewallがNATを行う場合は、NATルータと同じ問題が発生する。
  - この設置方法は避けた方が賢明。

11. Firewall併用時の注意点



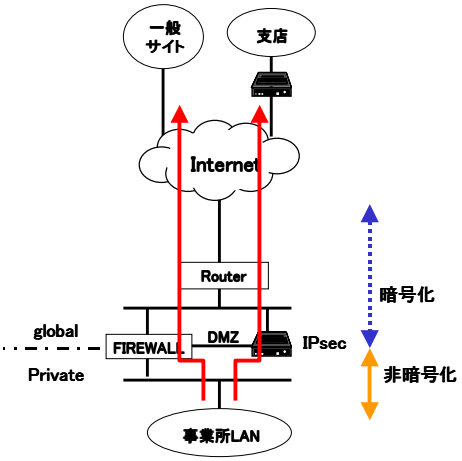
- Firewallの外側へIPsecを置く場合
  - Firewallに到達する前にデータは復号化されているのでFirewallのフィルタリング設定には影響を与えない。
  - FirewallがNATを行う場合は、IPsec gatewayから見ると事業所LAN上のホストがすべて同じIPに見えるので細かなセキュリティポリシーが設定できない。

11. Firewall併用時の注意点



- FirewallとIPsecを並列に置く場合
  - FirewallとIPsec gatewayを並列に設置し、用途に応じて経路を使い分ける。
  - 拠点間で暗号化通信をする時はIPsec gateway側の経路を使用し、Internet上の一般サイトへアクセスする時はFirewall側の経路を使用する。
  - ルータなどによる経路設定が必要。
  - Firewallの設定に影響をおよぼさない。
  - 他社との接続ではIPアドレスの重複に注意

11.Firewall併用時の注意点



- FirewallのDMZ経由でIPsecを並列に置く場合
  - 前ページの構成のバリエーションで、IPsec gatewayの内側のポートをFirewallのDMZに接続。
  - 前ページと同様に暗号化と非暗号化の経路を使い分けるが、そのルーティングをFirewallにさせる。

12. その他ソリューションとの併用の注意点

- QoSとの併用
  - 暗号データはQoSを適用できない場合がある。
  - QoSが適用される前に平文に戻るように設置位置に注意する。
- ウィルスチェックサーバとの併用
  - 暗号データはウィルスチェックを適用できない場合がある。
  - ウィルスチェックがされる前に平文に戻るように設置位置に注意する。

13. IPsec clientの仕様

- スループットはプラットホームの性能に左右される。
- 対応プラットホーム
- コンフィグレーション
  - 環境設定やポリシー変更の容易さ。
- アドレス管理
  - Internet経由のモバイル環境においてISPから割り振られるダイナミックアドレスとは別にユーザが管理するアドレスを付与できることが望ましい。

14. 管理機能

- 製品により管理機能が異なる。導入後のメンテナンスビリティに関わるので、要確認。
  - アドレス付与、ルール設定、バージョンアップ、状態監視
- 遠隔管理
  - SSL、SNMP、TELNET、独自プロトコル…
- コンソール
  - シリアル接続されたPC
- SAの状態管理
- SAの削除
  - コンソールから？
  - 特定のPhase2だけ削除可？

15. 障害対応

- ログ収集機能
  - コンソールログ、管理ソフトによる収集、Syslog、SMNP…
- 対応手順を事前に検討。
  - ログの確認、設定内容の確認、電源のoff/on…
  - 特に遠隔操作で対応できない場合も想定しておく。

16. 輸出規制に関する注意点

- IPsec製品は暗号機能を実装しているので輸出規制の対応となる。海外拠点に設置する場合は注意。
- 製品開発元の国の輸出規制および日本の輸出規制を、事前に確認必要がある。
- 輸入規制を取る国もある。
- 輸出規制以外に海外拠点への設置については、時差、言葉の壁、文化の違い等によりインストールや保守について十分に事前調整する必要がある。

17. 保守体制

- メーカや販売元の保守体制を確認。
  - 方法
    - センドバック、オンサイト
  - 対応時間
    - 平日9:00-17:00、365日24時間
  - 費用

IPsecによるVPN構築
第二部　おわり

株式会社ディアイティ