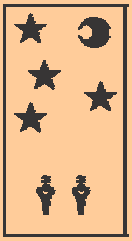
T20 : IPSec～技術概要とセキュアなネットワークの実現手法～

第2部　IPsecによるVPNの設計ポイント

2002/12/20

株式会社ディアイティ
山田　英史



内容

1. 要求仕様の確認
2. IPsec-VPNの設計ポイント
3. 実機試験

1. 要求仕様の確認

主な確認内容

- 代表的な1日のトラフィック状況を確認し、必要な帯域や機器の処理能力を把握。
- トラフィックの内容を確認し、パケット長やタイムアウトに関する留意点を洗い出す。
- 既存のネットワーク構成やアドレス体系を確認し、VPN導入に伴う作業工数を検討。
- どのホスト間でVPNを行なうのかを明確にして、セキュリティポリシーを作成。

要求事項の確認

- 導入の目的
- 既存ネットワークの構成（ルータ、NAT、Firewall等 既存機器の確認）
- WAN側の回線種、LAN側の回線種
- アドレス体系
- トポロジー（スター型、メッシュ型、一方向、双方向）
- VPNを利用するホストやネットワークの数
- VPNと一般インターネットアクセスの共存
- アプリケーションの種類
- 流れるプロトコルの種類
- パケットサイズ
- アクセス制限やNATなど
- 品質（タイムアウト、遅延、障害時の対応時間）
- トラフィック量の時間変化
- 管理者の有無
- 保守体制（24h365d xx時間内）
- 導入スケジュール
- 予算

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*

2. IPsec-VPN設計のポイント

ポイント

（1）トラフィックの質と量の把握
（2）既存ネットワークへの影響
（3）スループット
　　・パフォーマンス
（4）SAの検証
（5）経路上のルータの設定
（6）IPアドレスの運用
（7）平文と暗号通信の混在
（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・監視機能
（15）障害対応
（16）輸出規制に関する注意点
（17）保守体制

（1）トラフィックの質と量の把握

- トラフィック量は時間の経過によって変化する。
  - 日常業務のどの時間帯にトラフィックが最大になり、どのホストあるいはセグメントに集中するのかを把握 。
  - 流量に合わせたキャパシティを持つ製品を選択 。

（1）トラフィックの質と量の把握

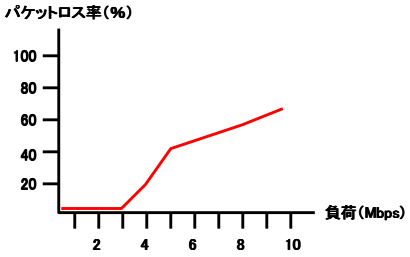
- 流れるパケットの大きさとアプリケーションのタイムアウトといった求められるトラフィックの質に注目 。
  - IPsec処理はオーバヘッドが大きい。
    - ショートパケットに弱いものもある。
    - Re-Keyの処理時間も考慮。

（2）既存ネットワークへの影響

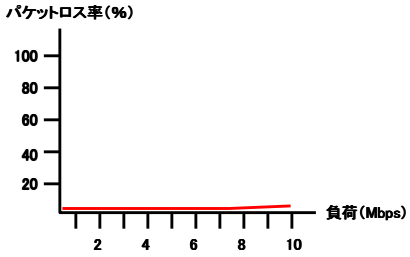
- IPsec-VPNを導入するネットワークを図に起こし、IPsec機器の設置箇所を吟味。特に既存のネットワークへの影響やサービスへの影響を考慮する。
- 既存の機器との併用
  - ファイアウォールやNATルータなどとの併用。

(3)スループット・パフォーマンス

- 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)



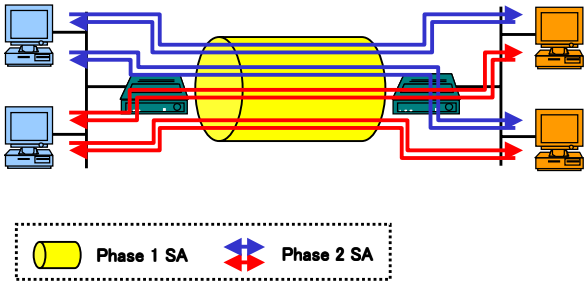
1440byte長パケット送出
(カタログスペック10Mbpsの製品)

(3)スループット・パフォーマンス

- 現実のパフォーマンス
  - Mbpsよりpps。
- SAの確立(Re-keyも)に要する時間
  - SA数によっては数分かかる場合もある。
  - アプリケーションのタイムアウトに注意。

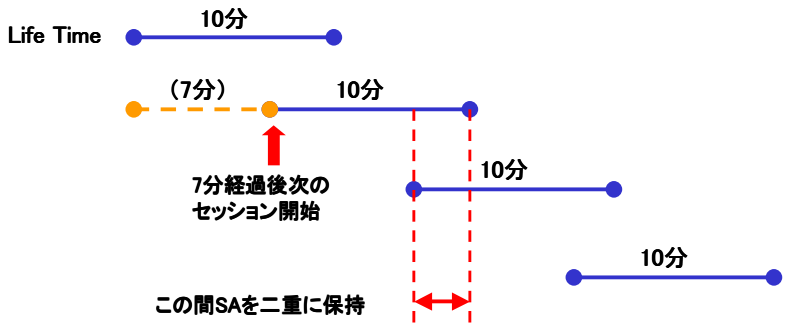
（4）SAの検証

- SA数
  - Phase 1は装置間毎＝対地に関係
  - Phase 2はターゲット毎（プロトコル毎に2本）＝ネットワーク規模に関連



（4）SAの検証

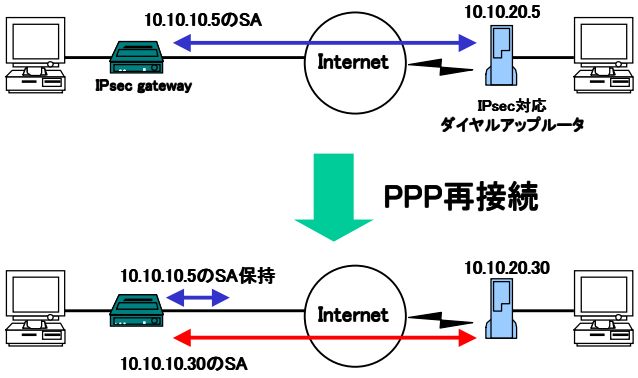
- Re-Key時のSA二重保持
  - 例えばフェーズ 2のLife Timeを10分と設定。
    - LifeTimeの何%で次のSAが準備されるかは製品によって異なる。
    - LifeTimeは経過時間以外にパケット数で設定できる製品も有り。



※フェーズ1はLife Timeの時点でいきなりRe-Key

（4）SAの検証

- リモートアクセス時のSA二重保持

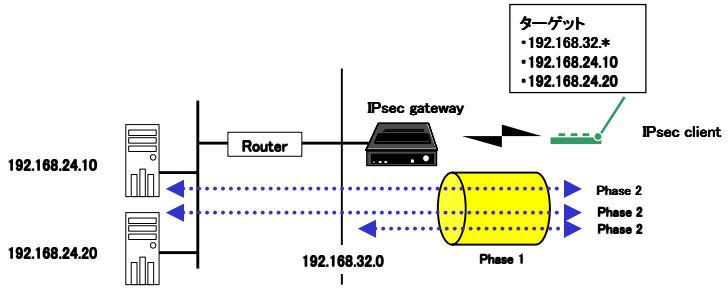


（4）SAの検証

- SAの最大値
  - “トンネル数”“セッション数”など各メーカにより様々。
    - Phase 1の数なのかPhase 2の数なのか。
    - Phase 2の上り下り2本を考慮していのか。
    - Phase 2 LifeTimeの重複は考慮しているのか。
    - 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。
  - Phase 1は実証試験が困難。
    - 装置を必要数用意することができない。

（4）SAの検証

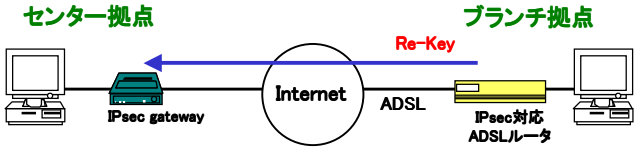
- SA数の調整



  - 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SA数が変わる。

（4）SAの検証

- LifeTimeの調整



・ダイナミックにアドレスが割り振られる拠点（ブランチ拠点）がイニシエータになるようにSA LifeTimeを短くする。

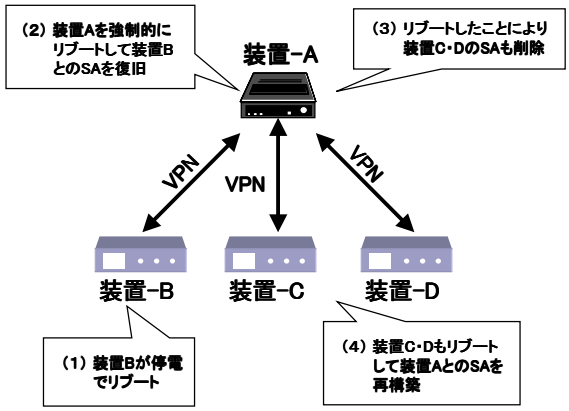
センター拠点＞ブランチ拠点

（4）SAの検証

- 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。
  - 他のトラフィックがある中でのRe-Keyはさらに時間がかかる可能性がある。

（4）SAの検証

- SAの復旧手順



・製品によりSA復旧の手順が異なる。
・異機種接続の場合は実機での検証が必要。
・手動で復旧が必要な場合は手順書等で明文化しておく。

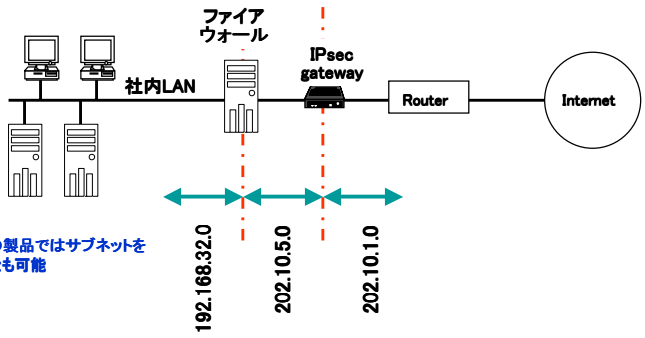
(5)経路上のルータの設定

- 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。

·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)
·認証プロトコルなど
  ·CA, LDAP
·製品固有の管理用プロトコルなど
  ·SSL, SNMP, FTP, 独自

(6)IPアドレスの運用

- ネットワークの分割
  - トンネルモードで使用の場合、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アドレスの運用

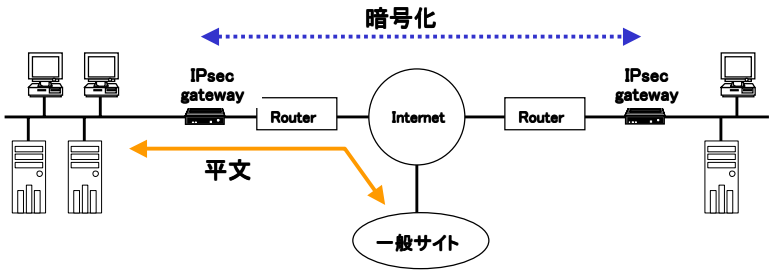
- IPアドレスの重複
  - BtoBなどエクストラネットで他社拠点と接続する場合は、双方のプライベートアドレスの重複を避ける。
    - グローバルアドレスを割り振る。
    - NATによりグローバルアドレスに変換。

（6）IPアドレスの運用

- モバイル端末に割り振るIPアドレスの保持
  - IPsec-DHCPなど方式の違いによりアドレスのプール数が異なる。
  - モバイル端末が同時に数百台がアクセスしてくる場合はアドレス空間に注意。

(7)平文通信許可時の注意点

- NAT機能、ルーティング機能、ファイアウォール機能の必要性。



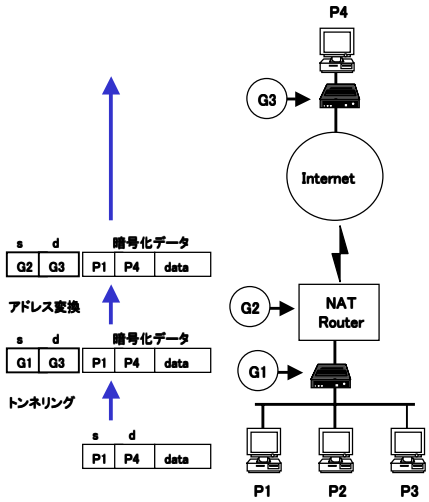
(8)フラグメンテーション

- IPsecヘッダが不可されることでパケット長が延長される。
  - フラグメンテーションによる通信効率の劣化に注意。
  - MTUの調整。

(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。

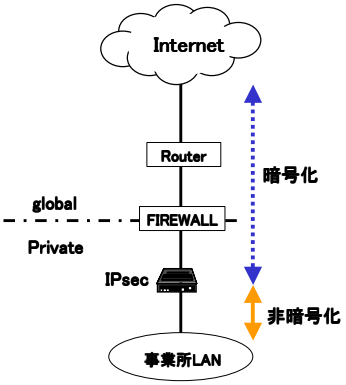
(10)NAT併用時の注意

- NAT併用時問題点の回避策
  - NATルータ自身がIPsecを実装。
  - NAT Traversalの標準化により問題解決。

(11)Firewall併用時の注意点

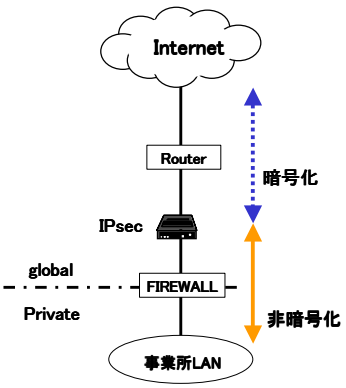
- ポート番号などの情報が欠けるため、暗号化されたデータはFirewallを通過出来ない場合がある。
- FirewallがNATをする場合の問題もある。

(11)Firewall併用時の注意点



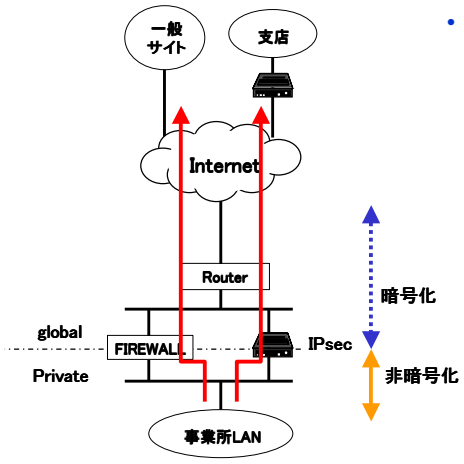
- Firewallの内側へIPsecを置く場合
  - 暗号化パケットを通過させるために様々な設定をFirewallに行う必要が有る。
  - FirewallがNATを行う場合は、NATルータと同じ問題が発生する。
  - この設置方法は避けた方が賢明。

(11)Firewall併用時の注意点



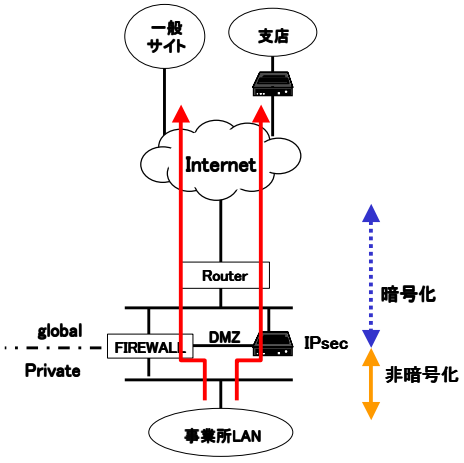
- Firewallの外側へIPsecを置く場合
  - Firewallに到達する前にデータは復号化されているのでFirewallのフィルタリング設定には影響を与えない。
  - FirewallがNATを行う場合は、IPsec gatewayから見ると事業所LAN上のホストがすべて同じIPに見えるので細かなセキュリティポリシーが設定できない。

(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。
    - IPsec-DHCP, PARなど

(14)管理・監視機能

- コンフィグレーション機能
  - アドレス付与、ルール設定、バージョンアップ、SAの状態管理、SAの削除操作
  - 操作環境
    - シリアル接続コンソール、Web、TELNET、独自管理ツール…

(14)管理・監視機能

- 状態管理・監視
  - SNMP、Syslog、Web、独自独自管理ツール
  - Pingによる死活監視

(14)管理・監視機能

- ログ機能
  - SNMP、Syslog、Web、独自管理ツール、シリアル接続コンソール

(15)障害対応

- ログ収集機能
  - ログ収集方法により精度が異なる。
  - 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。
- デバッグツールの有無

(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
  - 対応地域
  - 費用

3. 実機試験

実機によるパイロットテストの必要性

- 異なるメーカの製品を混在する場合（異機種間接続）。
- ADSLなど比較的新しい技術に適用する場合。
- 実際のアプリケーション環境下で使用するのに不安がある場合。
- 正常時の記録とエラーの記録。

Re-Key試験

- 異機種間試験では必要。
- Re-Keyが発生後も通信が途絶えることなく継続することを確認。
  - 装置AとBのSA Life Timeを長短混在させどの組み合わせで問題が出ないかを確認。
    - A=B、A>B、A<B
  - 試験通信はpingなどでOK。
  - ADSL等で一方のLifeTimeを故意に短くするような場合は実環境での試験が望ましい。

SA復旧試験

- 一報の装置のSAが削除された場合の復旧手順の確認とシステム与える影響の確認。
  - 装置間でpingをかけ続けた状態で、一方の装置を強制的にリブートしSAを削除、他の装置とのSA再構築の動作を確認。
    - 一報の装置が再起動したタイミングでSAが自動復旧するか否かを確認。
    - 自動復旧しない場合、もう一方の装置をリブートすることで復旧するか否かを確認。
    - 自動復旧しない場合、Re-Keyのタイミングで復旧するか否かを確認。

タイムアウト試験

- アプリケーション運用中にRe-keyが原因でタイムアウトしないことを確認。
  - 負荷発生装置（SmartBit等）で複数のSA（Phase 2）を確立しRe-keyに時間がかかる状態を故意に作る。
  - LifeTimeを短くしRe-Keyを頻発させる。
  - 上記の環境でアプリケーションを運用しある程度の時間問題なく運用できることを確認。

NAT越え試験

- NAT Traversalは製品により実装が異なるため、事前に試験をする。
  - NATルータ配下にIPsec Clientを複数台接続する場合、同時に通信できる台数を確認。
  - 実環境と同じアドレス体系で試験をする。
  - 実ネットワーク環境での試験も有効。

その他

- 製品依存の仕様は実機試験を行なう。
  - VoIPなどショートパケットが連続する場合のパフォーマンス試験。
  - 冗長構成試験。
  - PKIの運用試験。
    - 初期認証手順の確認。
    - CRL等の運用。

IPSec～技術概要とセキュアなネットワークの実現手法～

第2部 おわり

株式会社ディアイティ
山田　英史
eiji@dit.co.jp