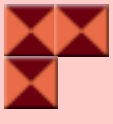
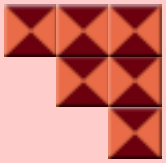



IPsecによるVPN構築　第三部

IPsec異機種間接続のポイント

2001/12/6

株式会社ディアイティ
技術部
山田　英史

内容

1. IPsec異機種間接続のポイント

IPsecによる異機種間接続のニーズ

- IPsec異機種間で接続の必要性

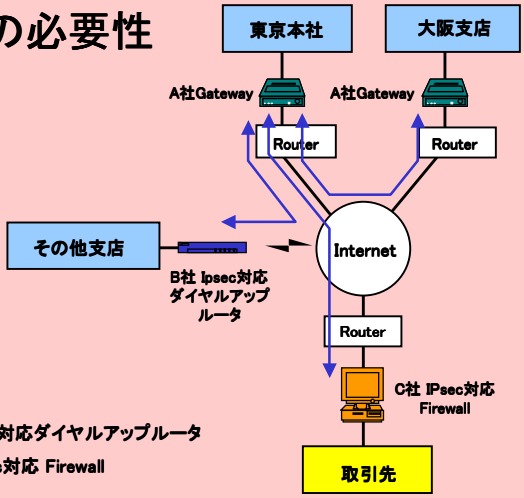
VPNがセキュリティ技術として普及

エクストラネットによる他社との間でVPN構築

IPsec異機種間接続の必要性

1. IPsec異機種間接続のポイント

- 異機種間接続の必要性



＜異機種間接続ペア＞

・A社IPsec GatewayとB社 IPsec対応ダイヤルアップルータ

・ A社IPsec GatewayとC社 IPsec対応 Firewall

1. IPsec異機種間接続のポイント

- 事前の調整項目
  - （1）IKEパラメータの調整
  - （2）認証方式の決定
  - （3）セキュリティポリシーの決定
  - （4）アドレスの重複回避

1. IPsec異機種間接続のポイント

- 日本ネットワークセキュリティ協会（JNSA）では以下のカテゴリで異機種間接続試験を実施。http://www.jnsa.org
  1. 基本試験
     - 1-1. 基本的な接続性試験
       - Pre-Sharedによる相互接続試験
       - Re-key後のSA継続の確認　その他
     - 1-2. 運用性確認
       - SA復旧試験
       - SA LifeTimeに関する試験
       - フラグメンテーション試験　その他
  2. オプション試験
     - 2-1. 基本的な接続性試験
       - CA認証による相互接続試験
       - NAT Traversal接続　その他
     - 2-2. 運用性確認
       - 性能試験　その他

2. IPsec異機種間接続の実際

2. IPsec異機種間接続の実際

- 異機種間接続の現状

メーカーによりIPsec実装レベルが異なる

実機による検証は必須

2. IPsec異機種間接続の実際

- 異機種間接続のための調査項目
  （1）パラメータの調査
  （2）安定性の調査（Re-Key試験）
  （3）SA復旧手順の確認

1. IPsec異機種間接続のポイント

（1）パラメータの調査

－IKEパラメーター一覧

＜IKEフェーズ 1＞

パラメータ種類	設定値など
Phase1モード	Main mode／Aggressive mode
暗号アルゴリズム	56bitDES／Triple-DES／他任意
ハッシュアルゴリズム	MD5／SHA-1
DHグループ	Gr1=768bit／Gr2=1024bit／Gr5=2048bit
認証用IDタイプ	IPアドレス／ドメイン名／メールアドレス／X.509DN／任意の名前
Phase1 SA LifeTime	任意の時間

1. IPsec異機種間接続のポイント

（1）パラメータの調査（続き）

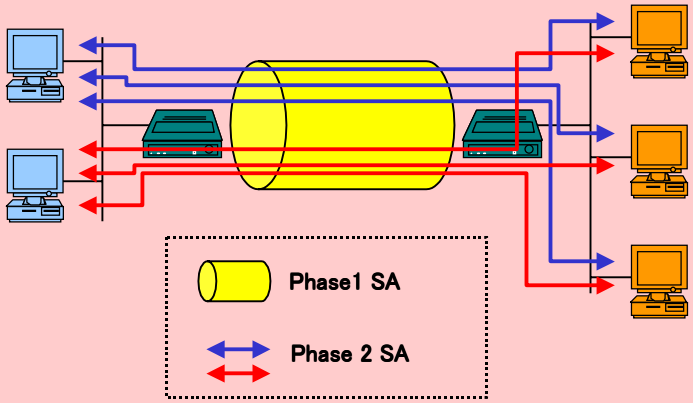
－IKEパラメーター一覧

＜IKEフェーズ 2＞

パラメータ種類	設定値など
Phase2モード	Quick mode
トランスフォーム ペイロード	ESPトランスポートモード／ESPトンネルモード
PFS（Perfect Forward Secrecy）	ON／OFF
Pase2 SA Life Time	任意の時間

1. IPsec異機種間接続のポイント

- SAの概念図



2. IPsec異機種間接続の実際

（1）パラメータの調査

- Ping等によるIKEの確立の確認
- InitiatorとResponderの方向性の有無の確認
- 接続可能なIKEパラメータの決定

2. IPsec異機種間接続の実際

（2）安定性の調査（Re-Key試験）

- FTP等による長時間通信の実施。
  - Re-Key発生後の通信継続の可否
- 数日間通信を続行。
  - パケットロス
  - スループット

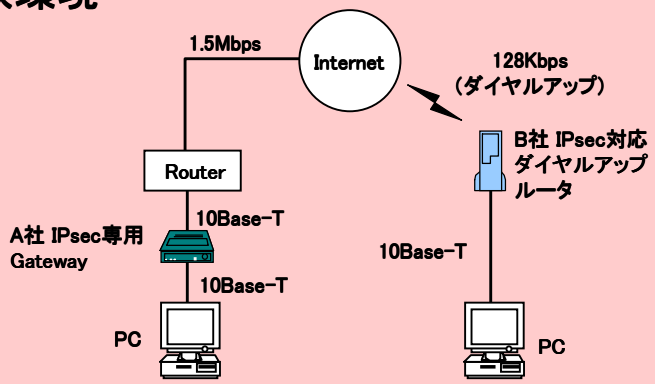
2. IPsec異機種間接続の実際

（3）SA復旧手順の確認

- 一方の装置が再起動した場合のSA復旧手順を確認
  - 大半は自動的に復旧できない

2. IPsec異機種間接続の実際

- IPsec異機種間接続試験の例
  - 試験環境



2. IPsec異機種間接続の実際

- IPsec異機種間接続試験の例
  - 試験の条件
    - アルゴリズム： 暗号=DES-CBC ハッシュ=MD5
    - IKEモード： Aggressive mode+Quick mode
    - DHグループ： 1
    - トランスフォーム ペイロード： ESPトンネルモード
    - IDタイプ： IPアドレス
    - PFS： ON
    - Key Life Time： Phase1 =10分、Phase2 =5分
    - 認証方式： Pre-Shared Key
    - Initiator： B社 Ipsec対応ダイヤルアップルータに固定

2. IPsec異機種間接続の実際

- IPsec異機種間接続試験の例
  - 試験１　IKEの確立確認
    - 結果：　ダイヤルアップルータからpingを打ち、上記パラメータ設定でSAの確立を確認できた。
  - 試験２　Re-Key試験
    - 結果：　SA確立後pingを継続し、その間に発生するRe-Keyの後も通信が継続することを確認した。

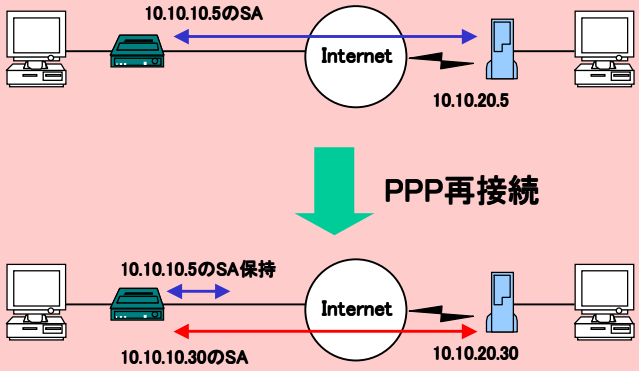
2. IPsec異機種間接続の実際

- IPsec異機種間接続試験の例
  - 試験3　回線切断後のSA復旧試験
    - 結果：　ダイヤルアップルータがPPPのタイムアウトした後の再接続の際、ダイヤルアップルータは新たなIPアドレスを得てSAの再構築をはかり、専用Gateway側はそれに答え新たなSAを確立。
    - この時専用Gateway側には旧SAが保持されたままになるが、Key Life Time経過後に削除される。

※このような特性は製品によって異なる。

2. IPsec異機種間接続の実際

- SAの二重保持



2. IPsec異機種間接続の実際

- IPsec異機種間接続試験の例
  - 試験5　IPsec専用Gateway再起動後のSAの復旧手順の確認
    - 結果：　専用Gatewayをリブートし SAを削除すると、ダイヤルアップルータ側にエラーが表示され、そのままの状態を放置するとKey Life Timeが経過するまでSAは再構築できない。
    - エラー検出時はすみやかにダイヤルアップルータ側もリブートし新たなSAの構築を行う必要がある。

3. IPsec異機種混在環境の注意点

3. IPsec異機種混在環境の注意点

（1）IKEパラメータに関する注意点
（2）セキュリティポリシーに関する注意点
（3）Re-Keyのタイミングに関する注意点
（4）認証方式の選択に関する注意点
（5）SA復旧手順に関する注意点
（6）3機種以上混在の場合の注意点
（7）バージョンに関する注意点

3. IPsec異機種混在環境の注意点

（1）IKEパラメータに関する注意点

– 利用環境で動作するパラメータ値が見つかればOK。

3. IPsec異機種混在環境の注意点

（2）セキュリティポリシーに関する注意点

– サブネット指定かホスト指定を事前に決定。

- 製品のサポート状況を考慮。
- SAのセッション数の上限を考慮。

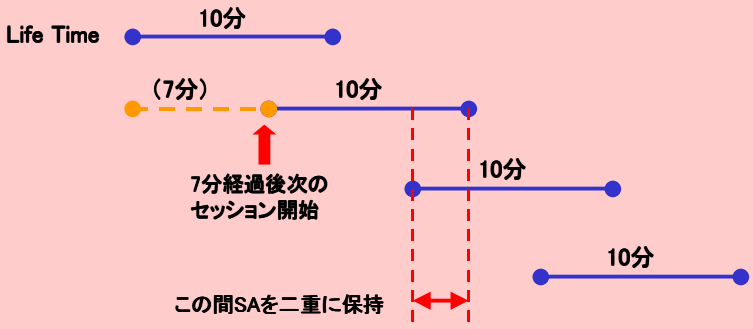
3. IPsec異機種混在環境の注意点

（3）Re-Keyのタイミングに関する注意点

- Key Life Timeを双方同じ時間に設定することを推奨。
- 製品の特性により一方が常にInitiatorになる必要がある場合はそちらのKey Life Timeを他方より短く設定。
- 製品によりRe-Key開始のタイミングが異なり、一時的にSAが二重に構築されるのでセッション数の上限に注意が必要。

3. IPsec異機種混在環境の注意点

- Re-Keyのタイミング
  - 例えばフェーズ 2のLife Timeを10分と設定



※製品により次セッションの開始のタイミングが異なる。

3. IPsec異機種混在環境の注意点

（4）認証方式の選択に関する注意点

- 異機種間接続ではPre-Sharedが主流。
- RADIUS認証やCA認証のニーズが高まる。
  - 問題点： 製品により実装レベルが異なる。
  - 問題点： ローカルCA間の相互認証の実績少ない。

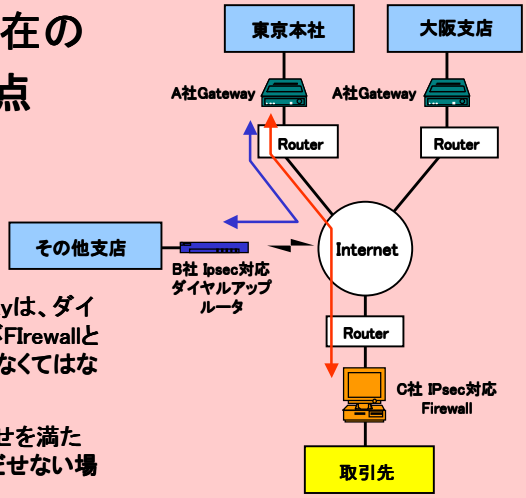
3. IPsec異機種混在環境の注意点

（5）SA復旧手順に関する注意点

- 自動的にSAが復旧するのは難しい。
- 運用でカバーすることが要求される。

3. IPsec異機種混在環境の注意点

（6）3機種以上混在の場合の注意点



東京本社にあるGatewayは、ダイヤルアップルータおよびFIrewallという2つの機種と接続しなくてはならない。

2組み以上の組み合わせを満たすパラメータ値が見いだせない場合がある。

3. IPsec異機種混在環境の注意点

（7）バージョンに関する注意点

- バージョンすることにより接続性が落ちる場合がある。

4. IPsec異機種間接続の今後

4. IPsec異機種間接続の今後

- IPsecの普及が異機種間接続の問題点を克服させる。
  - 現場で揉まれることにより、ベンダー間の調整が図られると予想。
- 不完全ながらも既に実績がある。
  - JNXでは異機種混在環境を構築。
  - 数百店舗規模のインターネット経由POS情報交換で実績有り。

IPsecによるVPN構築
第三部　おわり

株式会社ディアイティ