I P s e c

T10:IPSec ～技術概要とセキュアなネットワークの実現手法～

第二部 IPsec VPNの設計ポイント

2003/12/3

株式会社ディアイティ
セキュリティビジネス推進室
山田　英史

INTERNET WEEK 2003
2 - 5 December 2003 Yokohama / パシフィコ横浜

第二部の内容

1. IPsec VPNの設計ポイント
2. IPsec VPNの障害対応

1. IPsec VPN設計ポイント

1-1. 要求仕様の確認

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併用
- 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*

1-2. 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）フラグメンテーション
（8）認証方法の選択
（9）NAT併用の注意点
（10）Firewall併用時の注意点
（11）その他ソリューションとの併用の注意点
（12）IPsec clientの仕様
（13）管理・監視機能
（14）障害対応
（15）輸出規制に関する注意点
（16）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

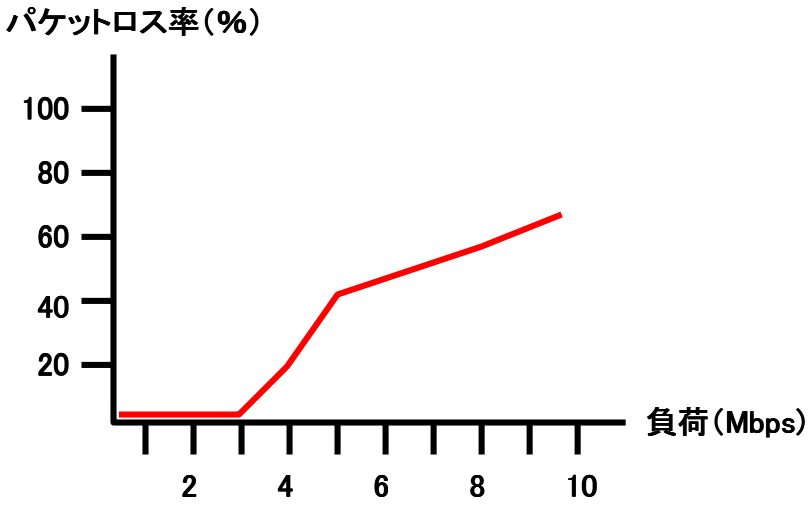
- 流れるパケットの大きさとアプリケーションのタイムアウトといった求められるトラフィックの質に注目
  - IPsec処理はオーバヘッドが大きい
    - ショートパケットに弱いものもある
    - Re-Keyの処理時間も考慮。

（2）既存ネットワークへの影響

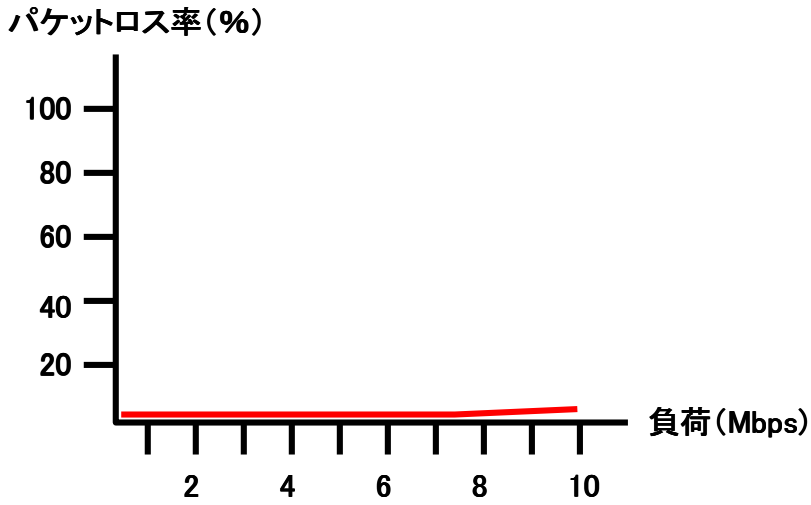
- IPsec-VPNを導入するネットワークを図に起こし、IPsec機器の設置箇所を吟味
- 特に既存のネットワークへの影響やサービスへの影響を考慮する
- 既存の機器との併用
  - ファイアウォールやNATルータなどとの併用

(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)



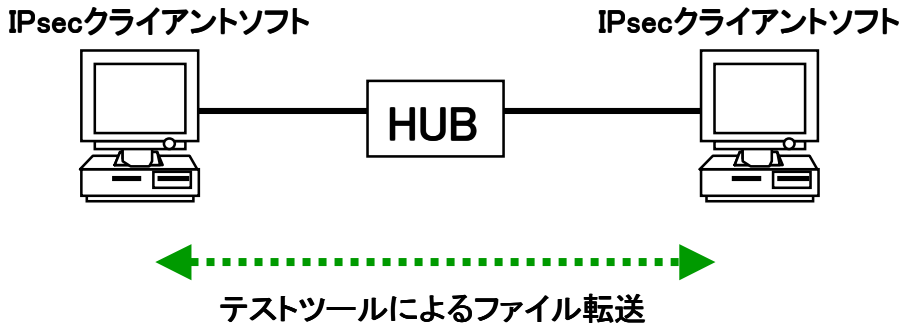
1440byte長パケット送出
(カタログスペック10Mbpsの製品)

(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

（3）スループット・パフォーマンス

- 実装による違い
  - Windows XP純正IPsecと市販のIPsecクライアントソフトの速度比較

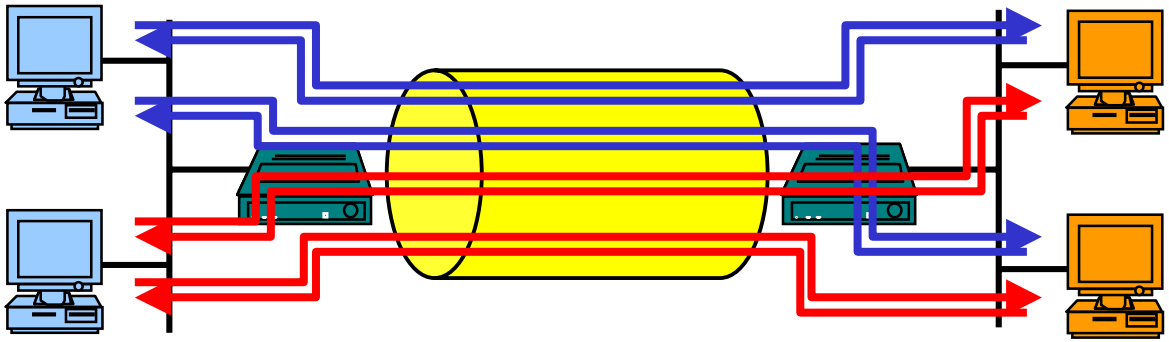


IPsec	平文	XP純正	市販ソフト
スループット（秒）	5	8	22

※ IKEログ保存を行うことで時間経過とともに速度の劣化が見られた。

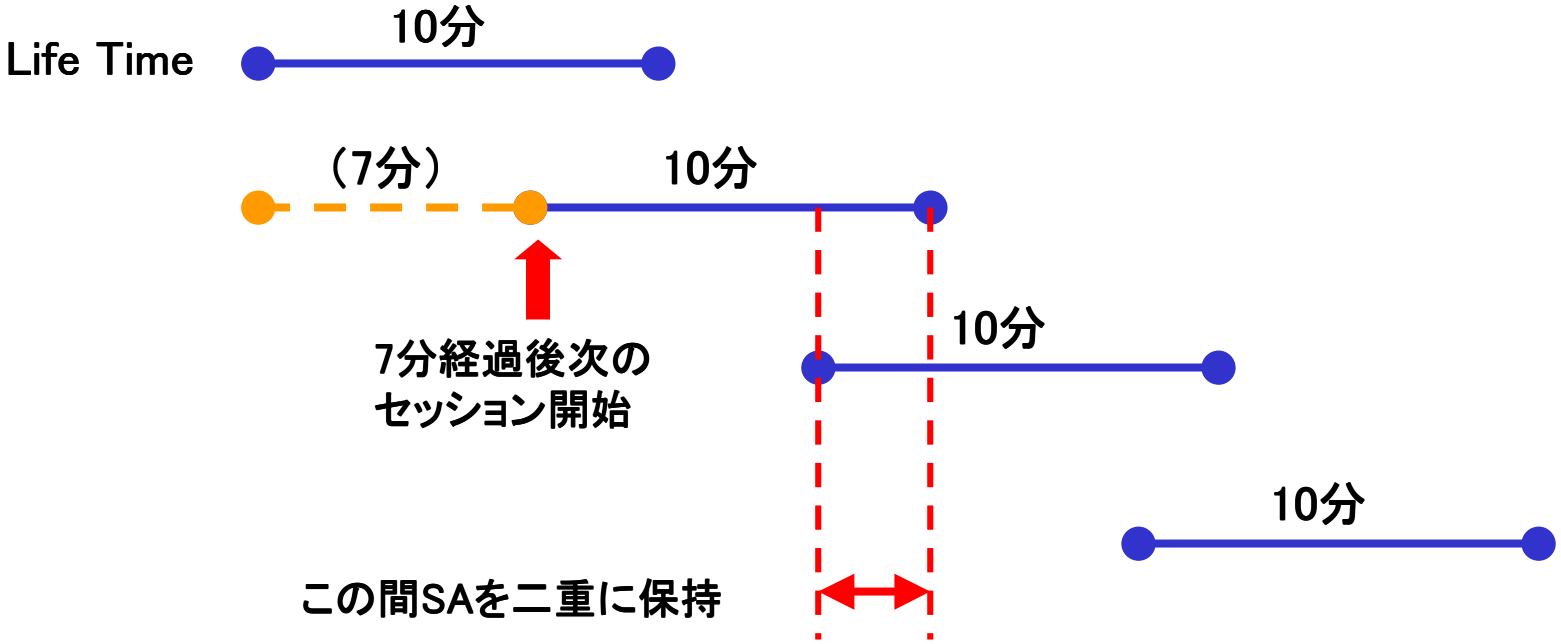
（4）SAの検証

- 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

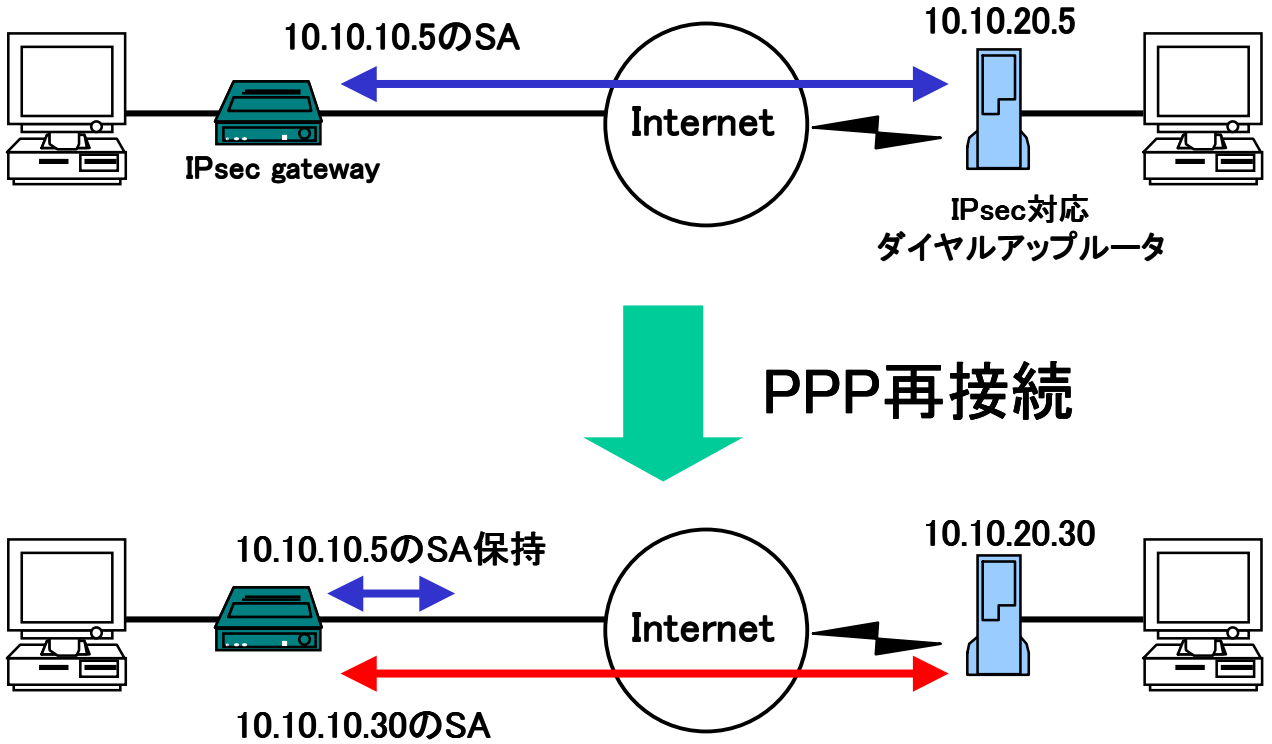
- Re-Key時のSA二重保持
  - 例えばフェーズ 2のLife Timeを10分と設定
    - LifeTimeの何%で次のSAが準備されるかは製品によって異なる
    - LifeTimeは経過時間以外にパケット数で設定できる製品も有り



※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

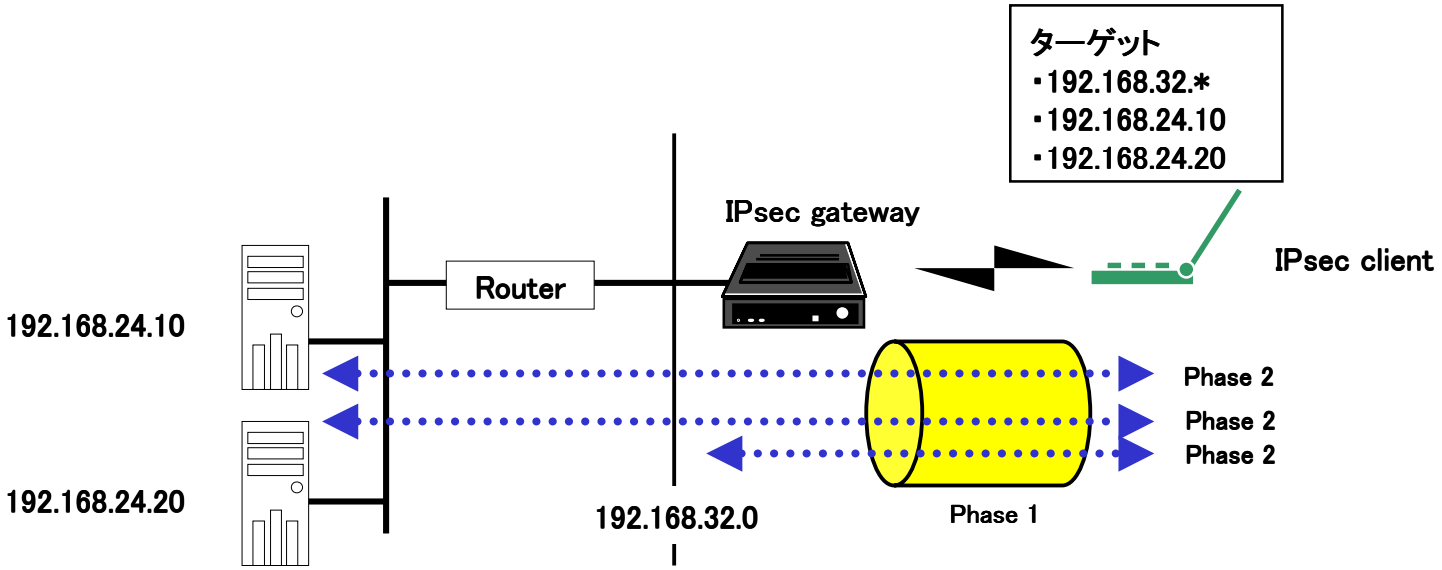


（4）SAの検証

- 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

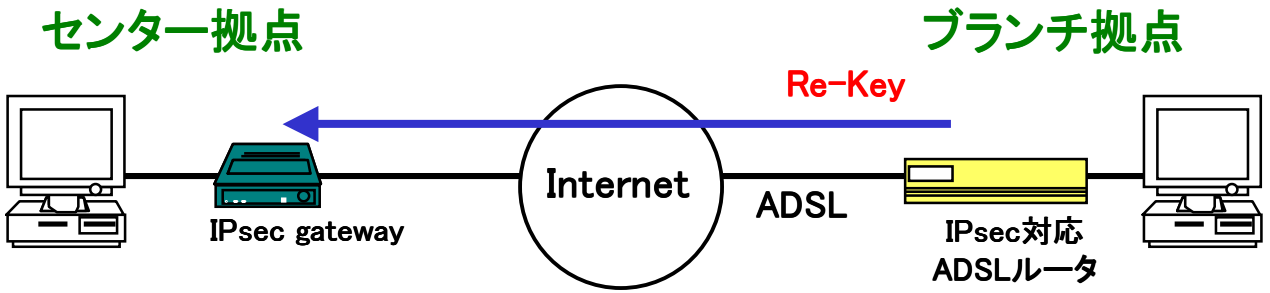
- SA数の調整



- 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

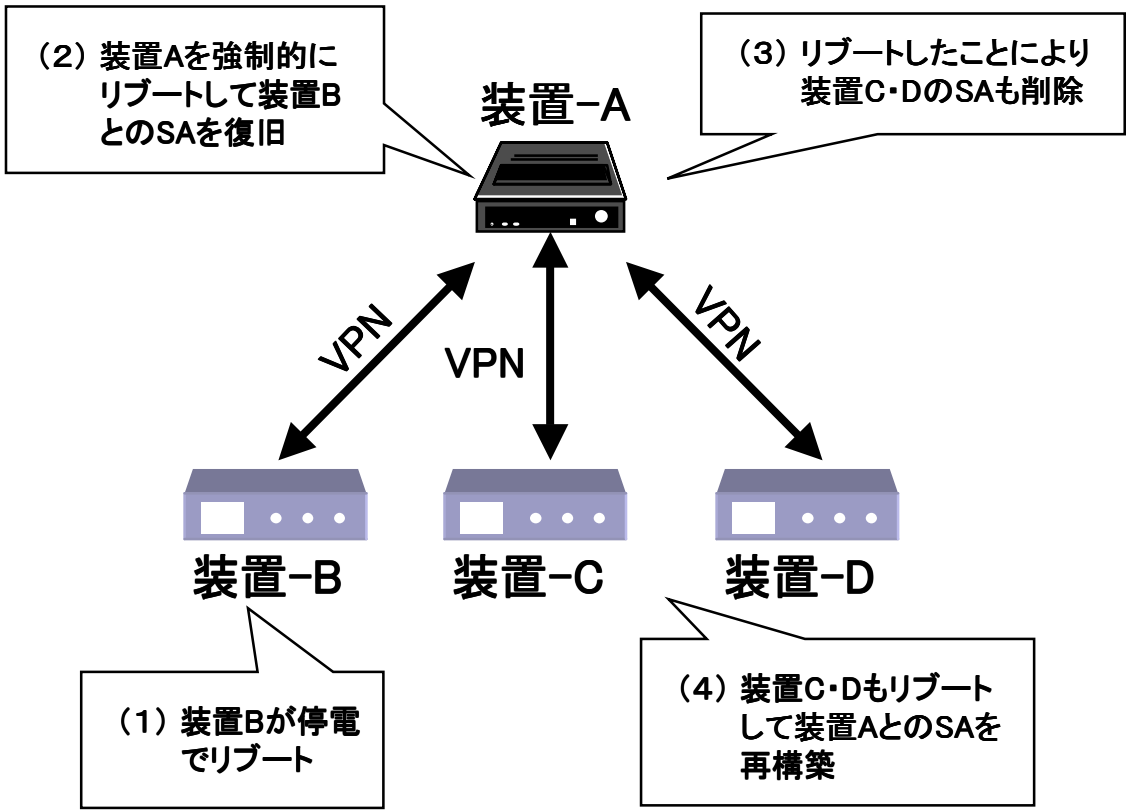
センター拠点＞ブランチ拠点

（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。

（4）SAの検証

- 異機種のSA復旧手順確認試験
  - AとBの2機種の場合

初期SA確立時の条件	SAの状態	リブートした側	pingした側	結果	備考
Aがイニシエーター	AのSAが残った状態	Bをリブート	Aからping	×	
		Bをリブート	Bからping	○	
	Aのフェーズ2のみ削除	Bをリブート	Aからping	×	Rekeyしない
		Bをリブート	Bからping	○	
	BのSAが残った状態	Aをリブート	Aからping	○	
		Aをリブート	Bからping	○	
	Bのフェーズ2のみ削除	Aをリブート	Aからping	○	
		Aをリブート	Bからping	×	90秒後、SA確立
Bがイニシエーター	AのSAが残った状態	Bをリブート	Aからping	×	
		Bをリブート	Bからping	○	
	Aのフェーズ2のみ削除	Bをリブート	Aからping	×	
		Bをリブート	Bからping	○	
	BのSAが残った状態	Aをリブート	Aからping	○	
		Aをリブート	Bからping	○	
	Bのフェーズ2のみ削除	Aをリブート	Aからping	○	
		Aをリブート	Bからping	×	90秒後、SA確立

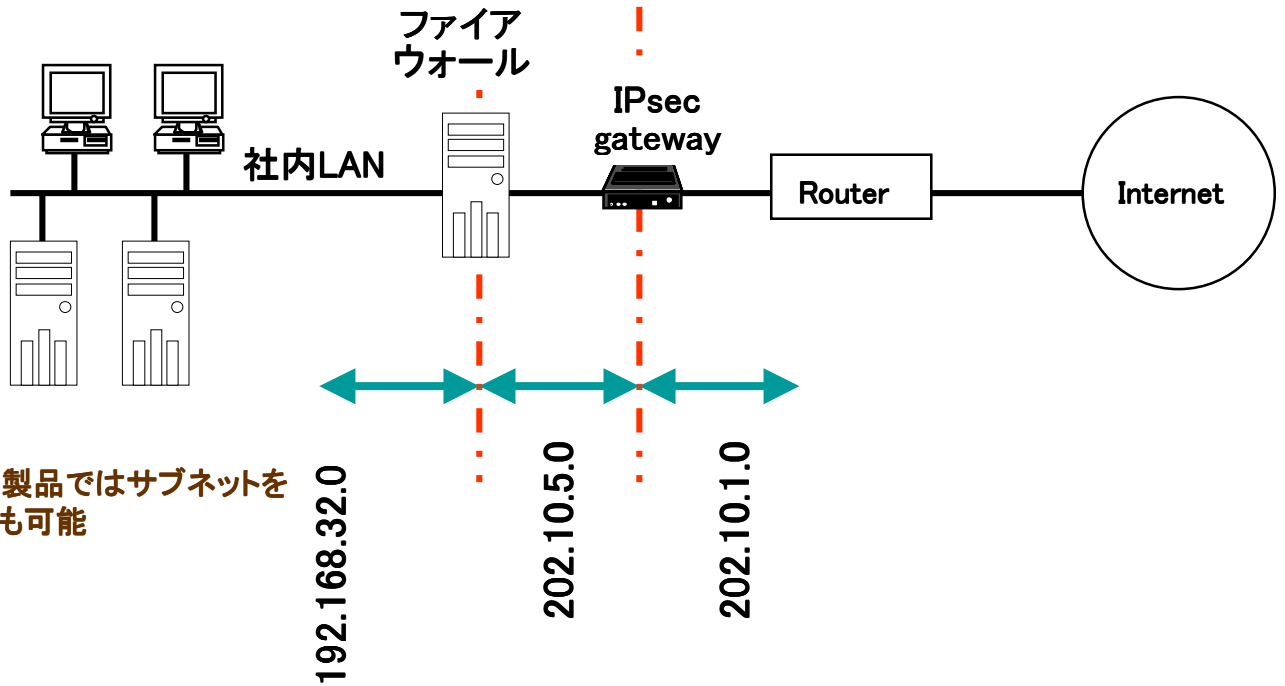
（5）経路上のルータの設定

- 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

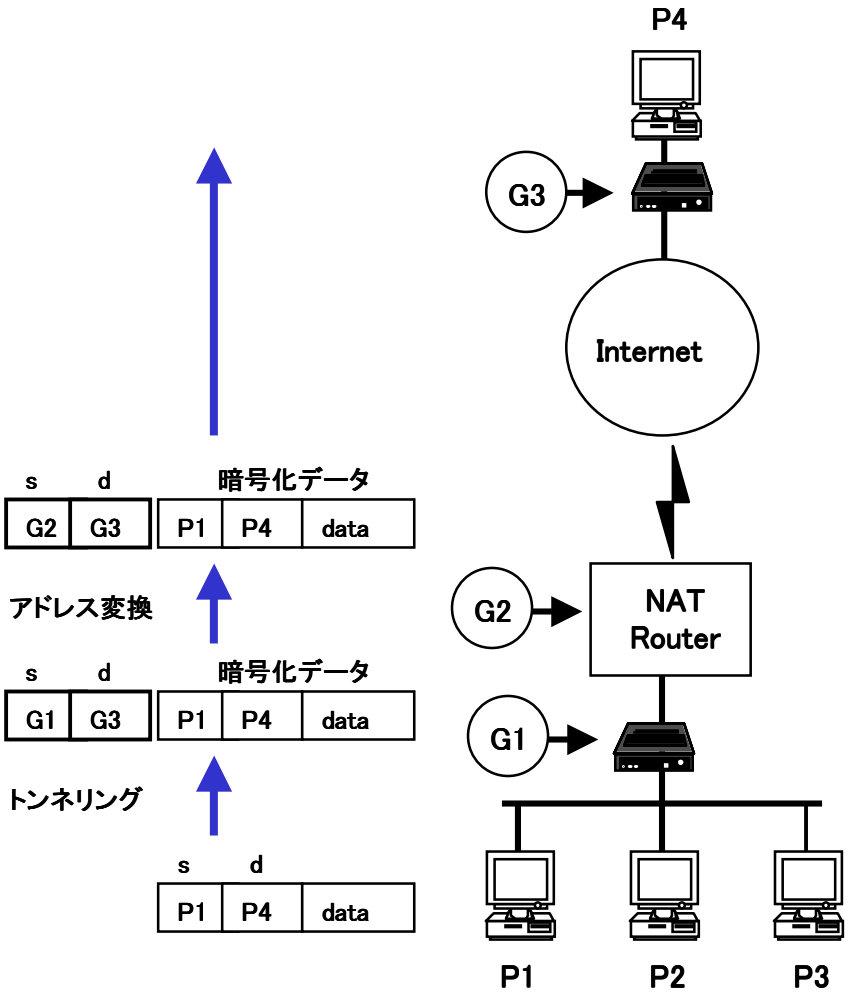
(7)フラグメンテーション

- 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(1380byte程度が良さそう)
  - DF=1にしてPMTUを通す

(8)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
    - 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
    - 製品によりサポート状況に差あり
  - CA認証
    - モバイルVPNおよび大規模VPN(n対n接続)に適する
    - 各種認証デバイス(ICカード等)による認証強化が可能
    - 製品によりサポート状況に差あり

(9)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

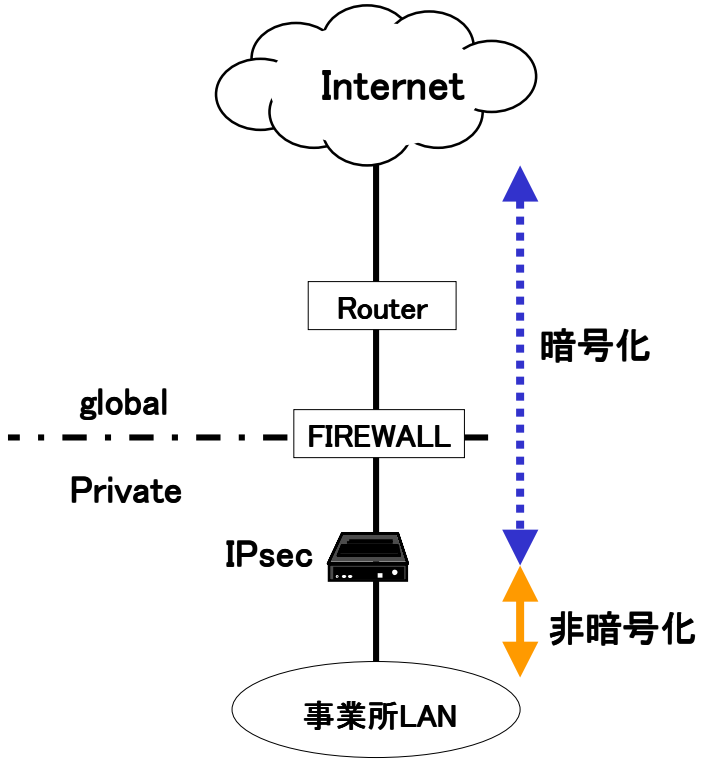
(9)NAT併用時の注意

- 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

(10)Firewall併用時の注意点

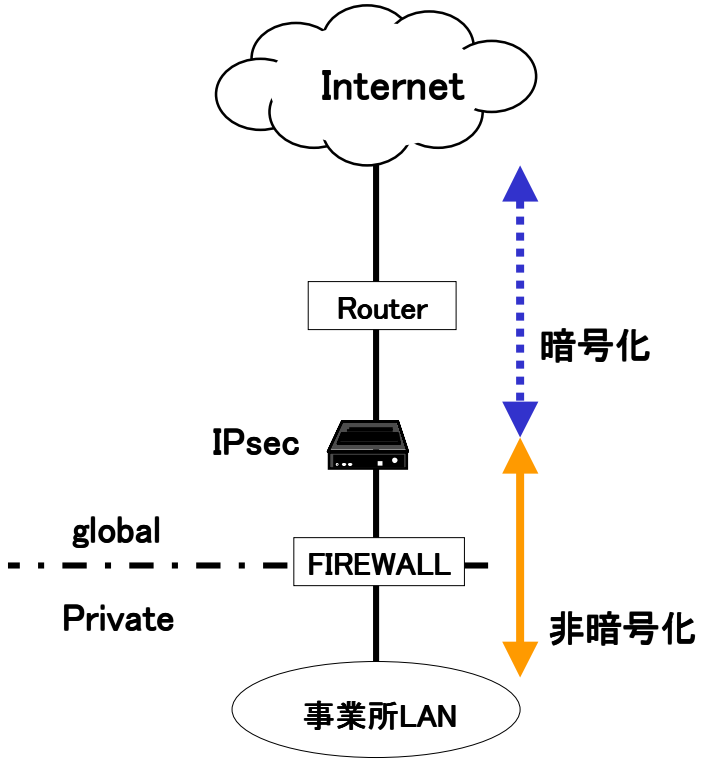
- ポート番号などの情報が欠けるため、暗号化されたデータはFirewallを通過出来ない場合がある
- FirewallがNATをする場合の問題もある

(10)Firewall併用時の注意点



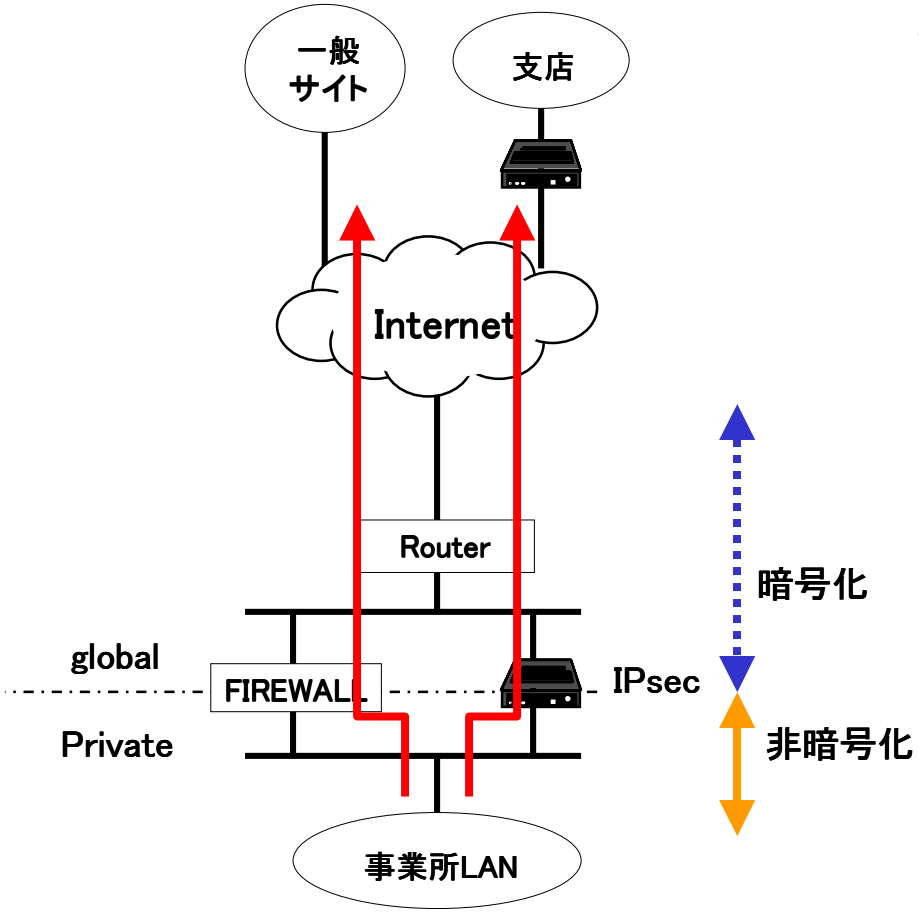
- Firewallの内側へIPsecを置く場合
  - 暗号化パケットを通過させるために様々な設定をFirewallに行う必要が有る
  - FirewallがNATを行う場合は、NATルータと同じ問題が発生する
  - この設置方法は避けた方が賢明

(10)Firewall併用時の注意点



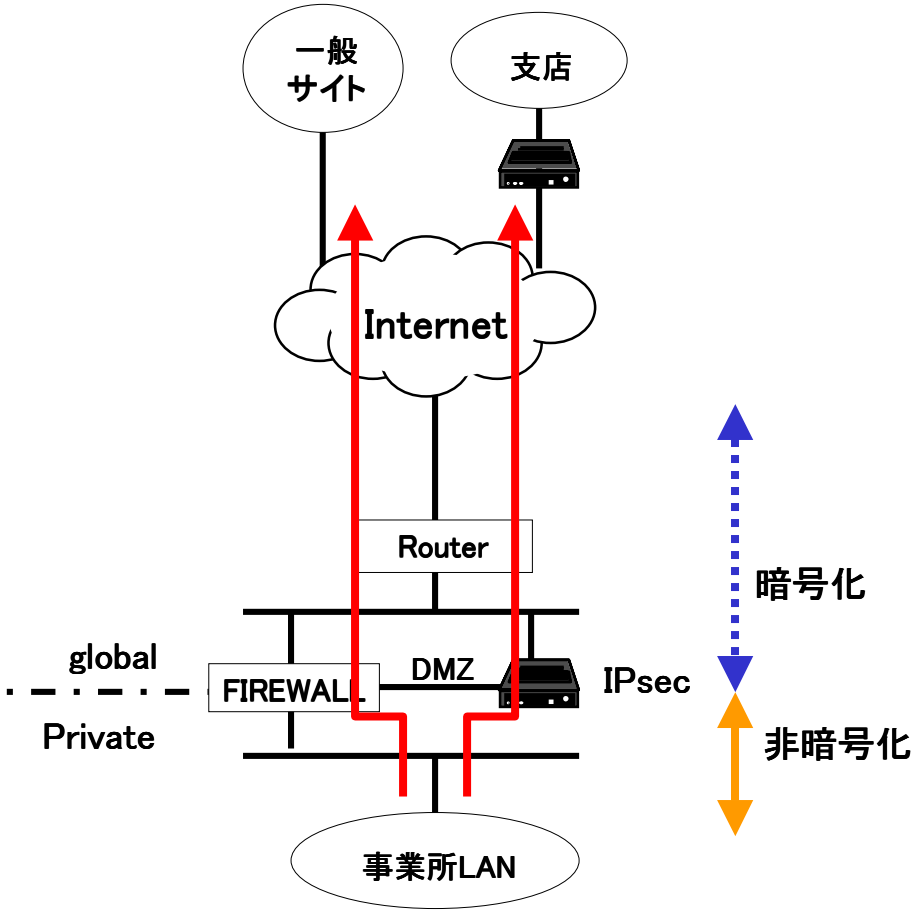
- Firewallの外側へIPsecを置く場合
  - Firewallに到達する前にデータは復号化されているのでFirewallのフィルタリング設定には影響を与えない
  - FirewallがNATを行う場合は、IPsec gatewayから見ると事業所LAN上のホストがすべて同じIPに見えるので細かなセキュリティポリシーが設定できない

(10)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

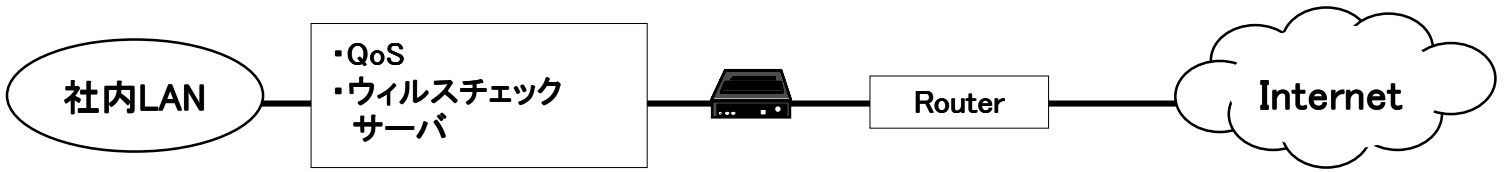
(10)Firewall併用時の注意点



- 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

（11）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行なわれる前に平文に戻るように設置位置に注意する



(12)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

(13)管理・監視機能

- コンフィグレーション設定機能
  - 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…

(13)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

(13)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

(14)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

(15)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、事前に確認する必要がある
- 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

(16)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

1-3. 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
- 標準外の機能を利用する場合（NAT越え、PKI…）
- 正常時の記録とエラーの記録

参考

NPO 日本ネットワークセキュリティ協会

http://www.jnsa.org

インターネットVPN WG

- 公衆無線LAN環境でのIPsec利用の調査
- NAT-Tに関する考察
- フラグメンテーションに関する考察
- IPアドレス重複に関する考察
- SAの説明

2. IPsec VPNの障害対応

2-1. 障害状況の把握

現状の把握

機器停止、機器の自動リブート、
一部通信の不具合、遅延、・・・

＜発生時の状況＞

発生日時
特定の時間帯に発生
決まった曜日に発生
特定の拠点に発生
特定のホストまたはネットワークに発生
特定のアプリケーションに発生
特定のオペレーションの後に発生

トラフィックの増加の後に発生ター
ゲットの増減の後に発生
回線の変更の後に発生
Re-Keyのタイミングで発生
CRLの更新後発生
アドレスの変更の後に発生
その他設定変更の後に発生

次ページへ

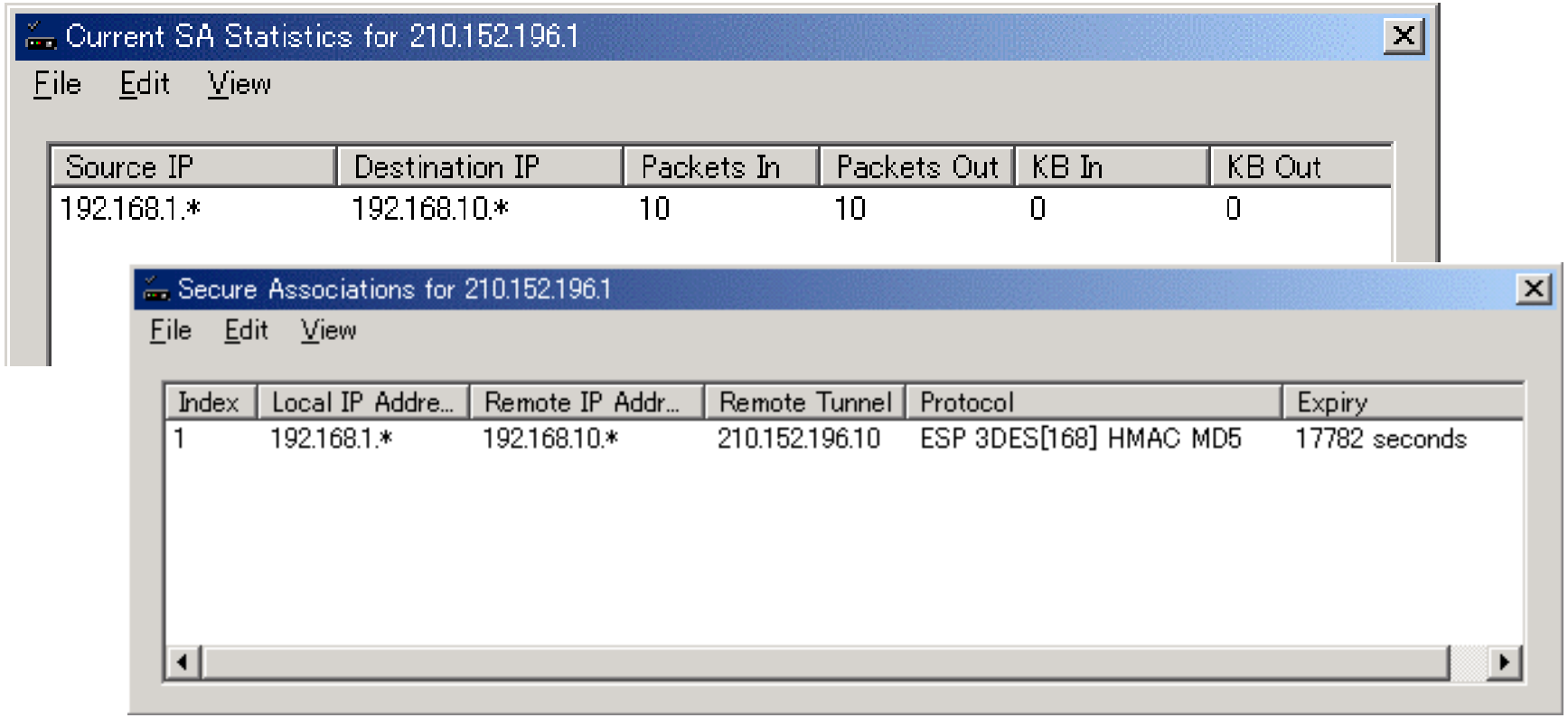
確認事項

前ページから

- ハードのインジケータ状態の確認
- SAの状態の確認
- パラメータ設定の確認
- セキュリティポリシーの確認
- ファームやソフトウェア バージョンの確認
- ログの確認
- Ping試験
- パケットアナライザーによるパケット評価
- デバックツールの使用

2-2. 正常な状態の把握

SAの状態



IKE確立までのログ

Session

Index	Date/Time	Reported By		Log Message
75	03/Dec/2002 07:21:11PM	Isakmp	ScSA	AddSa: SPIs:C0307A1D/2FEF5A47 Loc:192.168.1.* ← フェーズ 2の確立
				Rem:192.168.10.* (210.152.196.10) Prot:ESP-3DES[168]-HMAC-MD5 Exp:5:00:00
74	03/Dec/2002 07:21:10PM	Isakmp	cSA	Notify from 210.152.196.10: Initial Contact
73	03/Dec/2002 07:21:10PM	Isakmp	ScSA	AddPhase1: Rem:210.152.196.10, ID:"210.152.196.10", ← フェーズ 1の確立
				Cookies: 930802BDF812A961/D061A0255F9D657E Prot:DES[56]-MD5, Exp:23:59:59
72	03/Dec/2002 07:21:10PM	ShSecrt	ScSA	Found PW for: 210.152.196.10.
71	03/Dec/2002 07:21:09PM	Isakmp	ScSA	Got policy for peer:210.152.196.1, I am initiator, authentication: shared
70	03/Dec/2002 07:21:09PM	Isakmp	ScSA	Establish Request: 192.168.1.5 to 192.168.10.1 ← イニシエータとして動作
				≀
65	03/Dec/2002 06:52:15PM	Monitor	Evnt	Red port link: 10Mb HD
49	03/Dec/2002 06:37:18PM	Monitor	Evnt	Black port link: 10Mb HD
48	03/Dec/2002 06:37:18PM	Sonic	Init	LAN interface link status is supported.
47	03/Dec/2002 06:37:18PM	Monitor	Evnt	Gate is now Secure.
				≀
34	03/Dec/2002 06:37:08PM	Isakmp	ScSA	Default sa lifetime: 720
33	03/Dec/2002 06:37:08PM	Isakmp	ScSA	Current security level set to "Standard"
32	03/Dec/2002 06:37:08PM	Isakmp	Init	Initialized and running.
				≀
2	03/Dec/2002 06:36:59PM	RTC	Init	Initialized and running.
1	03/Dec/2002 06:36:59PM	RtcNVRA	Init	Initialized and running.

IKEネゴシエーション

インタフェースのリンクアップ

初期化と各種パラメータのセット

パケット

Capture021203.pkt

Packet	Source	Destination	Flags	Size	Absolute Time	Protocol	Summary
1	0[illegible]B	Ethernet Broadcast		64	19:14:37.505811	ARP Request	2[illegible]
2	0[illegible]D	0[illegible]B		64	19:14:37.509733	ARP Response	0[illegible]
3	0[illegible]D	0[illegible]B		64	19:14:37.510736	ARP Response	0[illegible]
4	IP-2[illegible]6.1	IP-2[illegible]6.10		177	19:14:37.518737	IP UDP	
5	IP-2[illegible]6.10	IP-2[illegible]6.1		177	19:14:37.542795	IP UDP	
6	IP-2[illegible]6.1	IP-2[illegible]6.10		218	19:14:37.560734	IP UDP	
7	IP-2[illegible]6.10	IP-2[illegible]6.1		218	19:14:38.049722	IP UDP	
8	IP-2[illegible]6.1	IP-2[illegible]6.10		138	19:14:38.540639	IP UDP	
9	IP-2[illegible]6.10	IP-2[illegible]6.1		138	19:14:38.575602	IP UDP	
10	IP-2[illegible]6.1	IP-2[illegible]6.10		322	19:14:38.621557	IP UDP	
11	IP-2[illegible]6.10	IP-2[illegible]6.1		322	19:14:38.667612	IP UDP	
12	IP-2[illegible]6.1	IP-2[illegible]6.10		98	19:14:39.662450	IP UDP	
13	IP-2[illegible]6.1	IP-2[illegible]6.10		130	19:14:41.812620	IP ESP	
14	IP-2[illegible]6.10	IP-2[illegible]6.1		130	19:14:41.819017	IP ESP	
15	IP-2[illegible]6.1	IP-2[illegible]6.10		130	19:14:42.311006	IP ESP	
16	IP-2[illegible]6.10	IP-2[illegible]6.1		130	19:14:42.314935	IP ESP	
17	IP-2[illegible]6.1	IP-2[illegible]6.10		130	19:14:42.909912	IP ESP	
18	IP-2[illegible]6.10	IP-2[illegible]6.1		130	19:14:42.913833	IP ESP	
19	IP-2[illegible]6.1	IP-2[illegible]6.10		130	19:14:43.491791	IP ESP	
20	IP-2[illegible]6.10	IP-2[illegible]6.1		130	19:14:43.495736	IP ESP	
21	IP-2[illegible]6.1	IP-2[illegible]6.10		130	19:14:44.007741	IP ESP	
22	IP-2[illegible]6.10	IP-2[illegible]6.1		130	19:14:44.011649	IP ESP	

Phase 1セッション（メインモード）

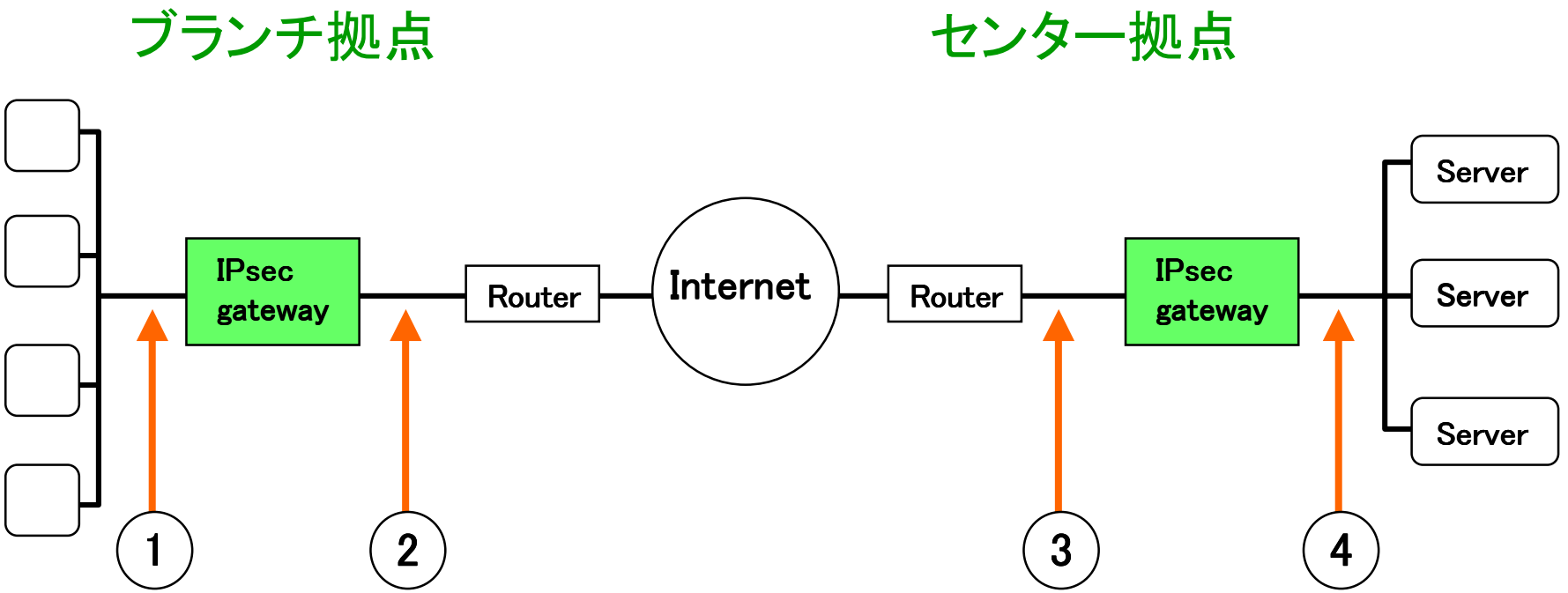
Phase 2セッション

暗号化通信

2-3. 障害切り分け

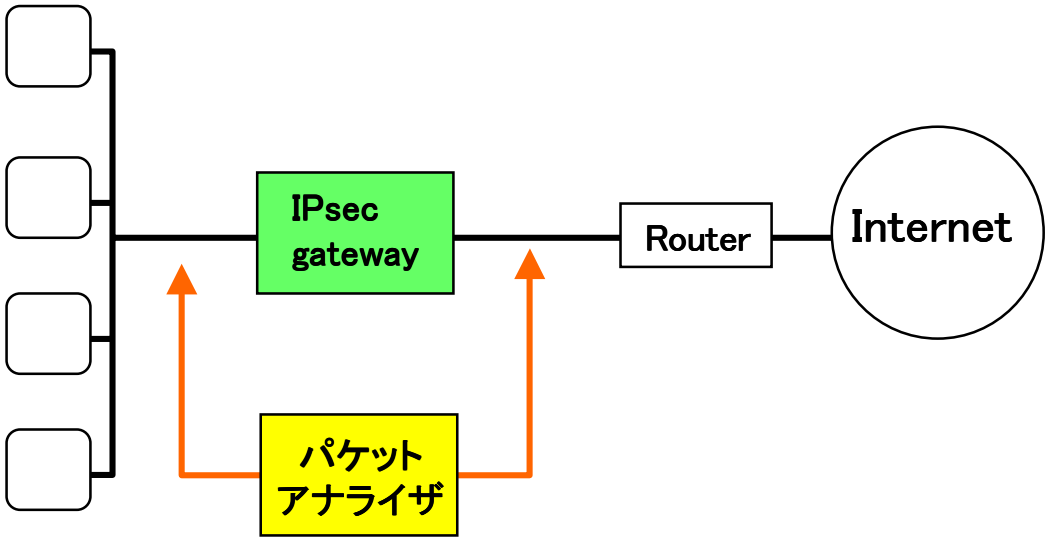
切り分け作業

パケットアナライザまたは試験用PCの接続箇所



切り分け作業

可能であればパケットアナライザ1台でgatewayを
挟んで両側の内外のパケットを同時に収集



記録時間にズレが無くなり、遅延などが把握しやすい

切り分け作業

- 障害が確認された拠点で現地調査
  - ブランチで障害発生時は同時にセンター側でも調査した方が良い
  - しかし、実際には人員の手配が付かずどちらか一方での作業になることが多い

Pingによる切り分け

- 経路上のどこに障害があるのかを予測
- 問題のあるホストまたはネットワークの特定
- IPsec gatewayの障害か否かの絞込み

例

- ブランチ拠点にあるクライアントからセンター拠点のあるサーバにアクセスできなくなったと想定

Pingによる切り分け

- 58ページの図においてブランチ側で切り分け作業を行なうと想定。
- ①にpingを送信するPCを設置
- ②にパケットアナライザを設置
  - ①からセンター内問題のサーバへpingを打つ。
  - ①からセンターの別のサーバやPCにpingを打つ。
  - ①からセンター IPsec gatewayの内部LAN側I/Fにpingを打つ。
  - ①からセンター側ルータへpingを打つ。
  - ①からセンター IPsec gatewayのInternet側I/Fにpingを打つ。
  - ②で収集したパケットの確認

Pingによる切り分け

- 確認事項
  - アプリケーションはだめでもpingは通るか
  - SAは確立しているか
  - IKEはどこで失敗するか
  - どことどこの間に問題がありそうか
- 原因箇所の絞込み
  - アプロケーション、ホスト、経路、IPsecの設定、IKEネゴ

Pingによる切り分け

- 前頁までの作業で障害箇所が見つからない場合
  - IPsec clientを実装した試験用PCを②に接続
    - ②から問題のサーバへpingを打つ
    - ②からセンター内の別のサーバやPCにpingを打つ
    - ②からセンター IPsec gatewayの内部LAN側I/Fにpingを打つ
    - 同様に②からブランチ内へもpingを打つ

Pingによる切り分け

- 確認事項
  - ブランチのIPsec Gatewayの外からなら問題ないか
  - SAは確立しているか
  - IKEはどこで失敗するか
  - どことどこの間に問題がありそうか

パケットアナライザによる切り分け

- IPsec gateway内部で何が起こっているのか＝ログの調査
  - ログ収集方法により精度が異なることに注意
- 外部で何が起こっているのか＝パケットアナライザによる解析
  - IPsec gatewayを挟むようにパケットアナライザを設置

パケットアナライザによる切り分け

- 58ページの図においてブランチ側で切り分け作業を行なうと想定
- ①②にパケットアナライザを設置
- 障害の起こるオペレーションを実施
- その際のパケットの収集とIPsec gatewayのログを照らし合わせて解析

パケットアナライザによる切り分け

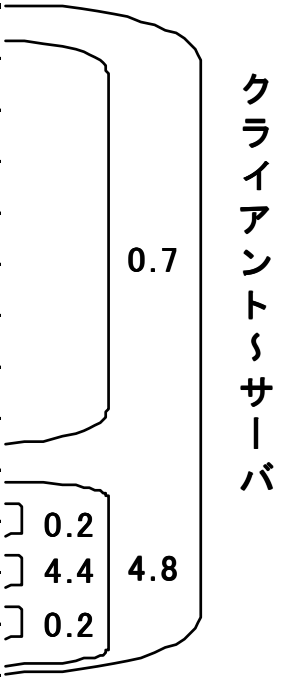
- 確認事項
  - IKEのどのプロセスで失敗するか
    - 何往復目で止まるか
  - はUDP500が経路上でフィルタされている可能性有り
  - 内部ログでエラーが記録されているか

パケットアナライザによる切り分け

- 確認事項
  - IKEは成功しているがパケットのやり取りができない。
    - ①と②でパケットにロスが確認できる。
    - ①と②で遅延が確認できる。

パケットアナライザによる切り分け

No.	発アドレス	着アドレス	byte	時間	サービス
1	IP-192.168.16.30	IP-192.168.16.35	154	30:32.8	IP UDP
2	IP-192.168.16.35	IP-192.168.16.30	206	30:32.8	IP UDP
3	IP-192.168.16.30	IP-192.168.16..35	226	30:32.9	IP UDP
4	IP-192.168.16.35	IP-192.168.16.30	226	30:33.0	IP UDP
5	IP-192.168.16.30	IP-192.168.16.35	138	30:33.1	IP UDP
6	IP-192.168.16.35	IP-192.168.16.30	106	30:33.1	IP UDP
7	IP-192.168.16.30	IP-192.168.16.35	930	30:33.3	IP UDP
8	IP-192.168.16.35	IP-192.168.16.30	338	30:33.3	IP UDP
9	IP-192.168.16..30	IP-192.168.16.35	98	30:33.5	IP UDP
10	IP-192.168.16.30	IP-192.168.16.35	306	30:33.8	IP ESP
11	IP-192.168.16.35	IP-192.168.16.30	90	30:34.0	IP ESP
12	IP-192.168.16.35	IP-192.168.16.30	114	30:38.4	IP ESP
13	IP-192.168.16.30	IP-192.168.16.35	90	30:38.6	IP ESP



- 確認箇所
  - 各パケット間の時間
  - ①と②で拾ったパケット間での遅延

2-3. 原因の特定

現地の切り分けで発見

- 切り分け作業で発生箇所を絞込み原因を特定
  - トリガーになるオペレーションを実施
  - 発生時間に合わせて精度を上げた再調査

擬似環境で再現試験

- 擬似環境で、予想される原因を試し、障害を再現
- 障害原因の予測
  - 高負荷
  - ショートパケット
  - SA数
  - Re-Key
  - 特定アプリケーション

デバッグ

- 実環境あるいは擬似環境で障害を再現しデバッグ
  - 共通秘密鍵がエクスポートできる機種ならデコード機能付きパケットアナライザ（松下電工 NetCocoon等）が使用可能
  - メーカのデバッグツールの使用
- 改善案を1つずつ段階的に試し、原因と改善策を決定

ご清聴ありがとうございました

株式会社ディアイティ
山田　英史
eiji@dit.co.jp