FUJITSU

shaping tomorrow with you

FUJITSU Network IPCOMとWindows AzureのIPsec接続について

2014年3月　富士通株式会社

Copyright 2014 FUJITSU LIMITED

はじめに

- 本資料は、Microsoft社のWindows Azureサービスを利用し、IPCOM EXシリーズとAzureサービス間で IPsec VPN接続を行う際の設定例を示した資料です。

- Windows Azureサービスは2014年1月時点のものです。

- IPCOM のファームバージョンはE20L30ですが、実際に利用するファームはシステム構築時の最新ファームを推奨します。

- 本資料の対象になるIPCOM EXシリーズ(※1)は以下です。

1100 SC	1300SC	2300SC	2500SC
1100 NW	1300NW	2300NW	2500NW
		2300IN	2500IN

※1…IPsec-VPNオプションを搭載しているもの

Copyright 2014 FUJITSU LIMITED

FUJITSU

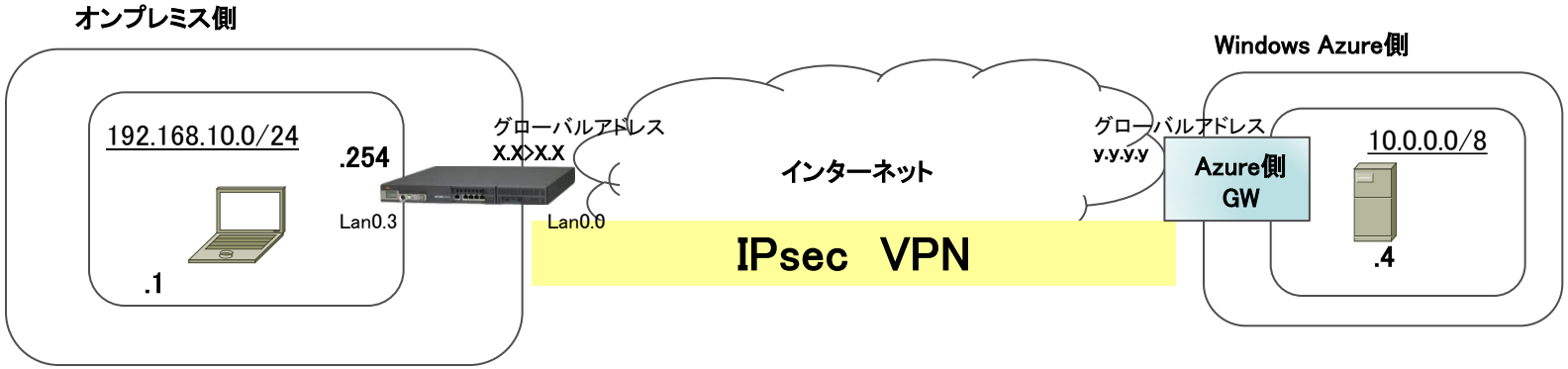
目次

Copyright 2014 FUJITSU LIMITED

1. 検証構成

以下に検証時の構成図とネットワークに関連する情報を記載します。

回線種別	Bフレッツ
IPCOM機種情報	IPCOM EX1100 SC
IPCOMファーム情報	E20L30NF0001



オンプレミス側　ネットワーク情報	
WAN側インタフェース	Lan0.0(※1)
WAN側アドレス	x.x.x.x
LAN側インタフェース	Lan0.3
LAN側セグメント	192.168.10.0/24
LAN側アドレス	192.168.10.254
端末アドレス	192.168.10.1

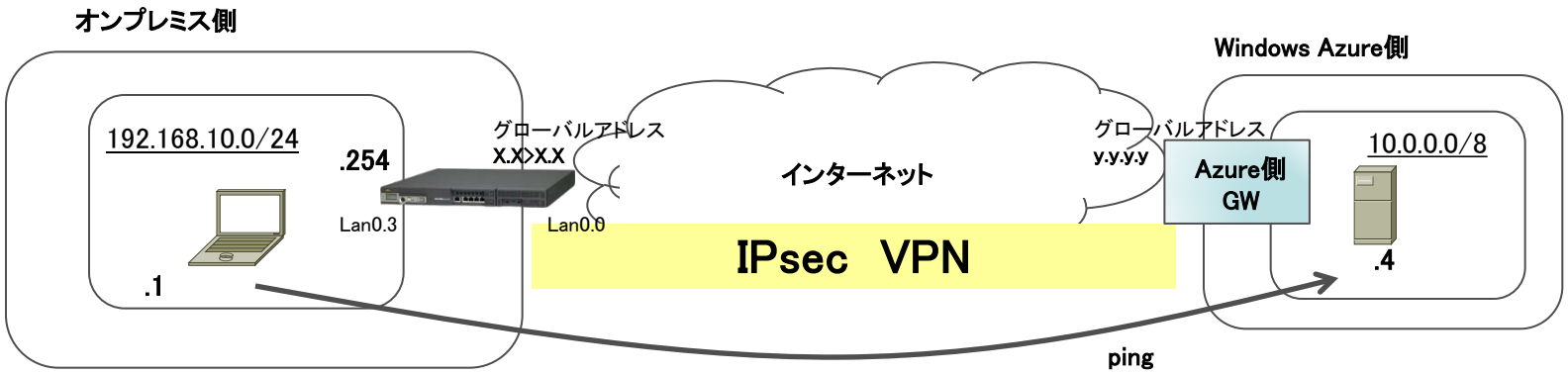
Azure側 GWネットワーク情報	
WAN側アドレス	y.y.y.y
LAN側セグメント	10.0.0.0/8
サーバアドレス	10.0.0.4

※1…実際にアドレスを持つインタフェースは
仮想インタフェースのppp0(PPPoE接続用インタフェース)

Copyright 2014 FUJITSU LIMITED

1. 検証構成

以下に検証時の構成図とIPsecに関する基本情報を記載します。
IPsecの情報は今回のサンプル定義で接続した際の情報です。



IPsec接続時の情報(今回の定義例で接続した場合の情報)		
IKEフェーズ1	鍵交換モード	メインモード
	暗号情報	AES-CBC256
	ハッシュ情報	HMAC-SHA1
	DHグループ	MODP1024
	生存期間	28800sec
IKEフェーズ2	暗号情報	AES-CBC128
	ハッシュ情報	HMAC-SHA1
	生存期間	3600sec
事前共有鍵	Azure側で生成されたキーに合わせる	

※暗号方式等は設定により、強度の高いものに変更可能です

IPCOMから見たピアアドレス	y.y.y.y (Azureのダッシュボード上で確認)
IPCOMから見た IPsec通信のアドレスレンジ	送信元:192.168.10.0/24 宛先:10.0.0.0/8

Azureから見たピアアドレス	x.x.x.x (IPCOMのshow interfaceで確認)
Azureから見た IPsec通信のアドレスレンジ	送信元:10.0.0.0/8 宛先:192.168.10.0/24

Copyright 2014 FUJITSU LIMITED

2. Windows Azureの設定

FUJITSU

Azureの仮想ネットワーク作成時に必要な設定

相手先アドレス	x.x.x.x(IPCOMのグローバルアドレス)
IPsec通信のアドレスレンジ	サーバ側(仮想マシン側)アドレス：10.0.0.0/8 IPCOM側の宛先アドレス　　：192.168.10.0/24

相手先(IPCOM)のグローバルアドレスは以下のコマンドで確認します

```
ipcom# show interface interface ppp0
 ppp0       MTU:   1492  <LINKUP,POINTTOPOINT>
   Type: ppp over ethernet
   Description:
   MAC address: 00:23:26:ee:01:9a
   IP address:                /32
   IP routing: enable
   Destination IP address:
   MRU: 1454
ipcom#
```

グローバル側のインタフェースを指定

IP address情報がここで確認出来る

Copyright 2014 FUJITSU LIMITED

2. Windows Azureの設定

- 仮想ネットワークの新規作成
  - ネットワークサービスから、「仮想ネットワーク」→「カスタム作成」を選びます。

Copyright 2014 FUJITSU LIMITED

2. Windows Azureの設定

- 仮想ネットワークの詳細の設定
  - 名前とアフィニティグループ名に任意の設定を入れます。ここでは、名前を「ipcom-vpn」、アフィニティグループ名を「ipcom1」と設定します。

Copyright 2014 FUJITSU LIMITED

2. Windows Azureの設定

- DNSサーバおよびVPN接続の設定
  - 必要に応じてDNSサーバを設定して下さい(今回は未設定)。今回構築するIPsecVPNはサイト間VPNなので、サイト間接続にチェックを入れて下さい。

Copyright 2014 FUJITSU LIMITED

2. Windows Azureの設定

- サイト間接続
  - 名前は任意の名前を入れて下さい。ここでは「ipcom-azure」とします。VPNデバイスのIPアドレスは、IPCOMのインタフェースに割り当てられたグローバルアドレスを設定します。アドレス空間は、IPCOM側のローカルセグメントのアドレスを入れます。ここでは192.168.10.0/24としています。

Copyright 2014 FUJITSU LIMITED

2. Windows Azureの設定

FUJITSU

仮想ネットワークアドレス空間の設定

- Azureの内側ネットワークの設定を行います。アドレス空間は10.0.0.0/8を指定します。アドレス空間を指定した後はサブネットを設定して、ゲートウェイサブネットを割り当てます。ここでは自動的に作成されたSubnet1(*1)と、「ゲートウェイの追加」ボタンで追加されたゲートウェイを使います。

※1…生成したSubnet1では10.0.0.0/11が割り当てられますが、IPsecの対象はあくまでアドレス空間で設定した10.0.0.0/8を指定します。

Copyright 2014 FUJITSU LIMITED

2. Windows Azureの設定

ゲートウェイの追加

- ゲートウェイを追加します。「ネットワーク」→「ダッシュボード」からゲートウェイの追加から、静的ルーティングの追加のボタンを押します。ゲートウェイの作成には暫く時間がかかります。

ゲートウェイ作成前

ゲートウェイ作成中

Copyright 2014 FUJITSU LIMITED

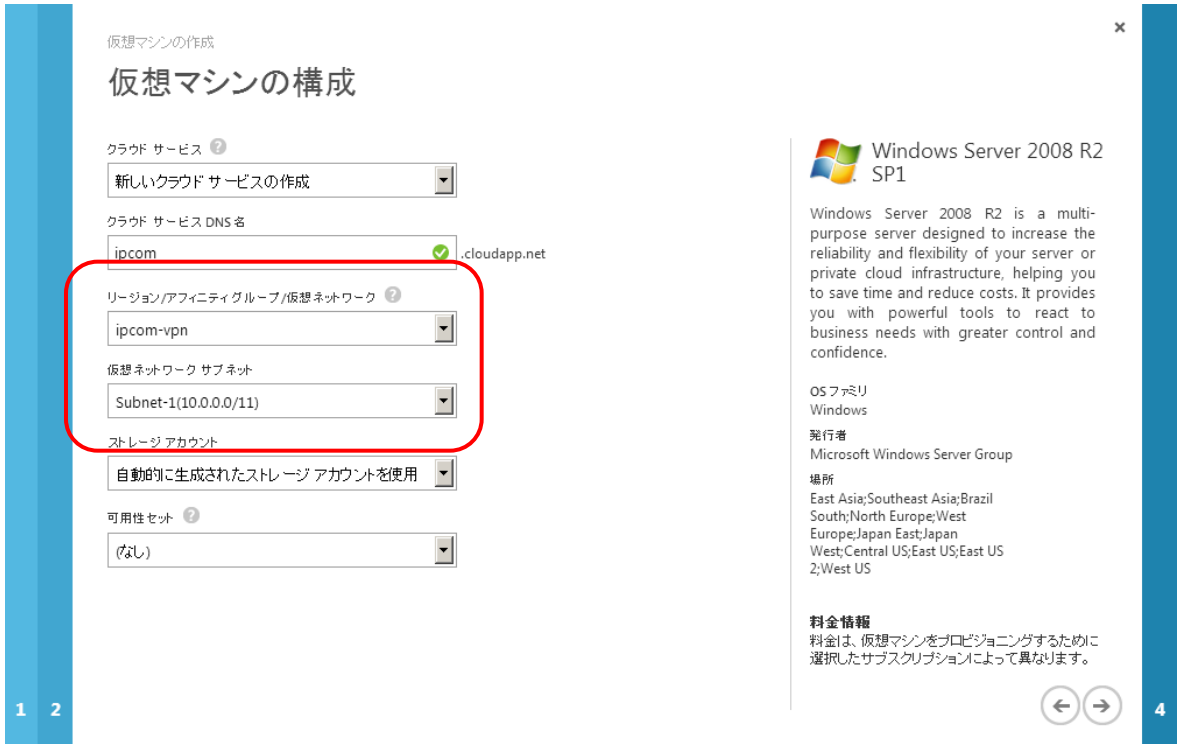
2. Windows Azureの設定

- ゲートウェイが作成したら、①アドレス、②共有キーを確認します。この2つは、IPCOMの設定を行う上で必要な情報です。Azure側の仮想ネットワーク作成は以上です。

Copyright 2014 FUJITSU LIMITED

2. Windows Azureの設定

- 最後に疎通確認用のサーバを作成します。先程作成した仮想ネットワークの後ろに仮想マシンを作成します。仮想マシンをギャラリーから作成する際、作成した仮想ネットワーク(ここではipcom-vpn)を使い、サブネットが意図したアドレスになっているかを確認して下さい。



Copyright 2014 FUJITSU LIMITED

3. IPCOM EXの設定

FUJITSU

- 次にIPCOMの設定を行います。以下に設定に必要な内容を洗い出します。

設定項目	設定値	備考
相手先アドレス	y.y.y.y	P12で確認した内容
事前共有鍵	XXX	P12で確認した内容
IPCOMから見た IPsec通信のアドレスレンジ	送信元アドレス：192.168.10.0/24 宛先アドレス　：10.0.0.0/8	IPCOMのローカルネットワークが送信元、 Azureのローカルアドレスが宛先アドレス
接続に利用するインタフェース	lan0.0	定義上はppp0とする

- その他
  - 今回はデフォルト値を利用し、最小の設定で接続しています。必要に応じて鍵交換モードやIPsec上の設定を変更して下さい。
  - 今回はIPsecの定義のみ掲載していますが、別途ファイアウォールや攻撃防御の設定を行って下さい。特に今回のサンプルコンフィグでは、全ての通信を許可する設定になっているので、必ず必要な通信のみ許可するよう設定を行って下さい。

Copyright 2014 FUJITSU LIMITED

3. IPCOM EXの設定

FUJITSU

IPsecの設定

今回の定義例では、「IKEルール」「IPsecルール」「事前共有鍵」を作成します

コマンド設定例	説明
【IKEルールの設定】 ike rule 100 　set-peer ipv4 y.y.y.y interface ppp0	IKEルールの設定 フェーズ1におけるポリシーを設定するルールです。今回はピアアドレスと接続インタフェースのみ指定し、他の設定値はデフォルト値を利用します。
【IKE事前共有鍵の設定】 ike pre-shared-key ipv4 y.y.y.y key XXXXX interface ppp0	事前共有鍵の設定 相手先アドレスをikeのIDとして、Azure側で生成された共有鍵を設定します。
【IPsecルールの設定】 ipsec rule 100 　class-map ipsec1 　set-peer ipv4 y.y.y.y interface ppp0	IPsecルールの設定 フェーズ2におけるポリシーを設定するルールです。今回はピアアドレスと接続インタフェースと「rule 100」に適用するアドレスレンジを指定して、他の設定値はデフォルト値を利用します。
【クラスマップの設定】 class-map match-all ipsec1 　match source-address ip 192.168.10.0/24 　match destination-address ip 10.0.0.0/8	IPsec通信のアドレスレンジ設定 ipec rule 100に適用されるアドレスレンジを設定します。必ず対向装置の設定と整合性を合わせる必要があります。今回の例では、Azure側から見ると、通信の送信元は10.0.0.0/8で、宛先が192.168.10.0/24なりますが、IPCOM側から見るとこれは逆になるので、逆に設定しています。

Copyright 2014 FUJITSU LIMITED

3. IPCOM EXの設定

- 以下のコンフィグはあくまで試験的に接続する為だけのコンフィグです。**インターネットに接続する場合は、別途ファイアウォール機能や攻撃防御機能、管理者ユーザのパスワード設定等を行って下さい。**

```
fixup protocol dns 53/udp
fixup protocol ftp 21/tcp
fixup protocol http 80-83/tcp
fixup protocol http 8080-8083/tcp
fixup protocol https 443/tcp
access-control default-accept
protect checksum-inspection enable audit-normal
ike rule 100
    set-peer ipv4 y.y.y.y interface ppp0
     exchange-mode main
!
ike pre-shared-key ipv4 y.y.y.y key XXX interface ppp0
Interface lan0.0
!
interface lan0.3
    ip address 192.168.10.254 255.255.255.0
    ip-routing
!
interface ppp0
    ip address auto
    ip-routing
    ppp user-name 123@456.78
    ppp password aaaaaaa
    ppp dns-server auto
    ppp mru 1454
    ppp adjust-mss auto
    ppp add-routers
    ppp-link lan0.0
```

pppoe接続に必要なIDとパスワードを設定

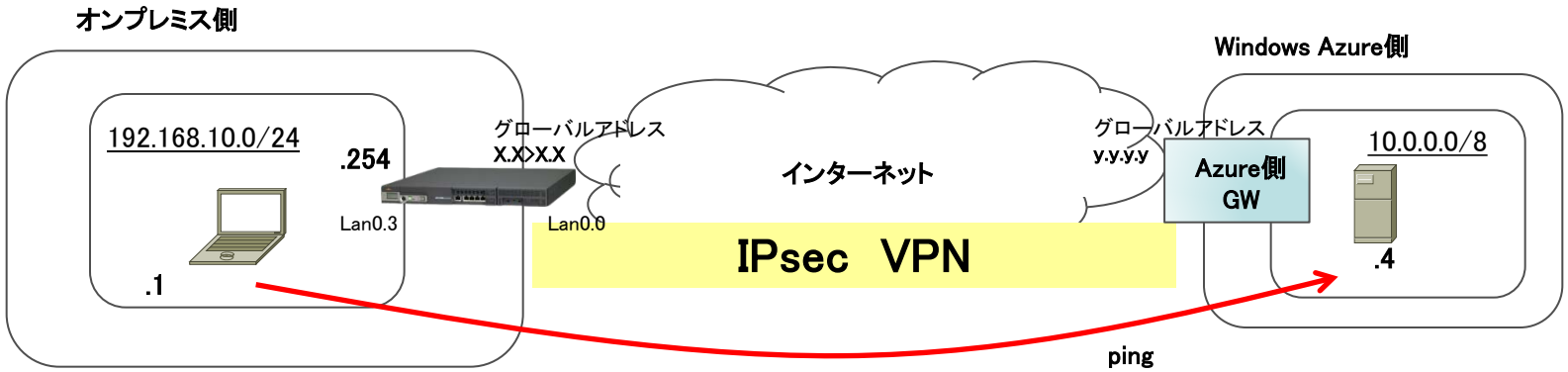
```
!
ipsec rule 100
    class-map ipsec1
    set-peer ipv4 y.y.y.y interface ppp0
!
class-map match-all any
    match any
!
class-map match-all ipsec1
    match source-address ip 192.168.10.0/24
    match destination-address ip 10.0.0.0/8
!
user-role administrator
    description "Default user role"
    display-name "IPCOM administrators"
    match user admin
!
user-role remote
    description "Default user role"
    display-name "IPCOM access via network"
    match user admin
!
user-role user
    description "Default user role"
    display-name "IPCOM operators"
!
user admin
    valid
```


Copyright 2014 FUJITSU LIMITED

4. 通信成功時の確認

テスト通信

- 以上の作業で必要な設定が完了しました。この状態でオンプレミス側の端末からAzure側に作成したサーバにping疎通確認を行います。

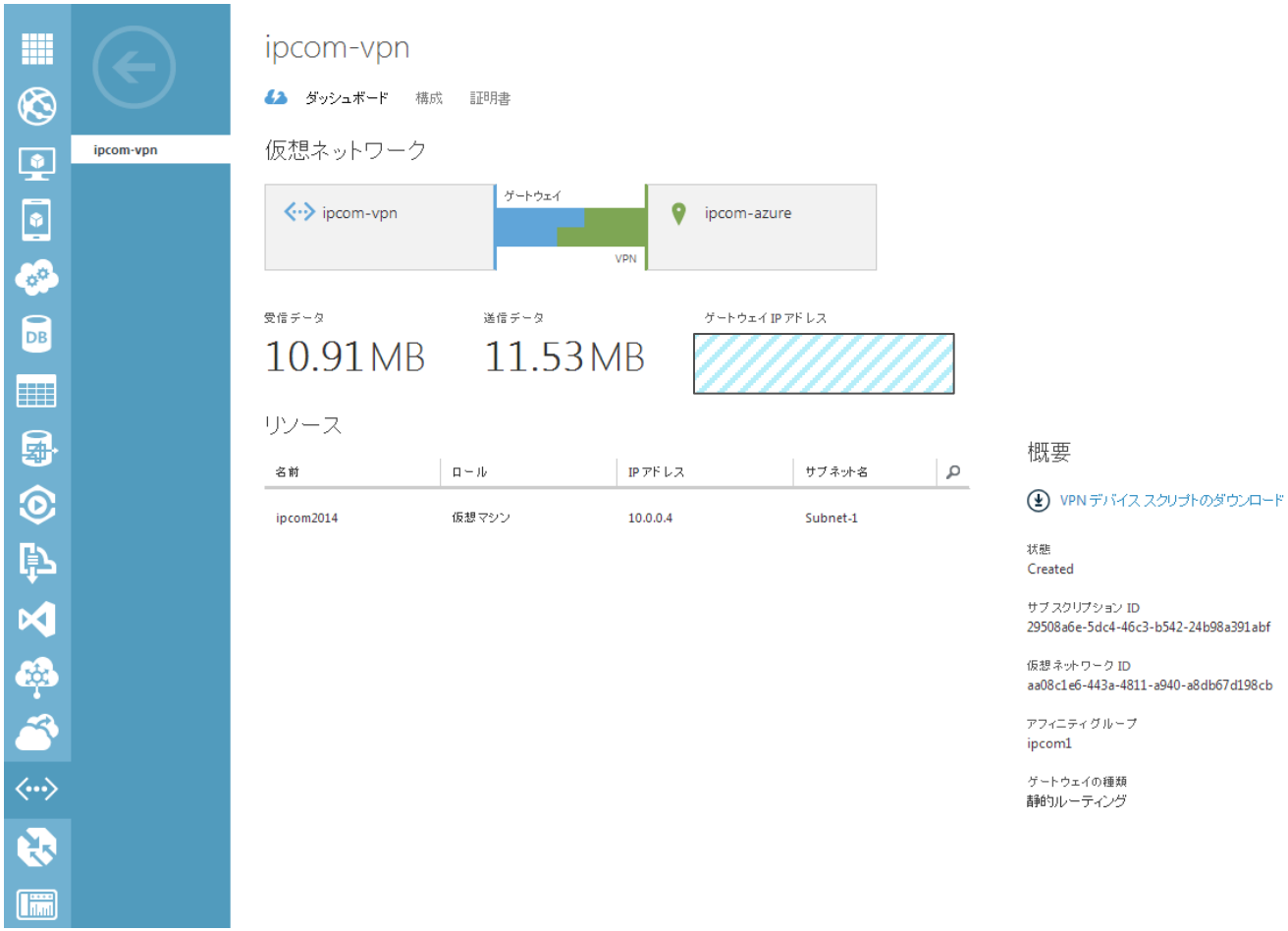


なお、Azure側のサーバはping疎通試験を行う為に予めリモートデスクトップ接続を行い、サーバ上のファイアウォールを無効にして、ping応答出来る状態に設定している状態です。

Copyright 2014 FUJITSU LIMITED

4. 通信成功時の確認

- Azure側では以下の「仮想ネットワーク」→「ダッシュボード」の画面から、接続が行われデータが流れている事が確認出来ます。



Copyright 2014 FUJITSU LIMITED

4. 通信成功時の確認

- IPsecのSAが確立されて通信が成功すると、以下のコマンドでIPsecに関する統計情報を確認する事が出来ます。

コマンド名	出力内容
show ike summary	ike確率情報の統計情報 detail等の引数で詳細情報を出す事も可能
show ipsec-information summary	IPsecトンネルに関する統計情報 detail等の引数で詳細情報を出す事も可能

- これらのコマンドの結果が出力されない場合は、設定やネットワーク設定に問題がある場合があります。IPsecの設定に問題がある場合は、「show logging message」コマンドの結果、”IKE”や”IPsec”という機能メッセージ単位でログが上がります。

Copyright 2014 FUJITSU LIMITED

4. 通信成功時の確認

- IPsecのSAが確立されて通信が成功すると、以下のような出力結果になります。

show ike summary

```
ipcom# show ike su show ike summary
[ISAKMP SA Information]
[No 0001]
    (Current ISAKMP SA)
    Local-IP(ppp0: [redacted])
    Peer-IP([redacted])
    Side(Initiator), Status(Established), Commit-bit(OFF)
    Cookie(f807d0616b97221d):(b0c9bf9de2a405e3)
```

show ipsec summary

```
ipcom# show ipsec su show ipsec summary
[IPsec SA Information]
[No 0001]
    (Current IPsec SA)
    Mode(tunnel)
    Local-IP(ppp0: [redacted])
    Peer-IP([redacted])
    Direction(IN), Protocol(ESP), Spi(3188694197,0xbe0f9cb5)
    Source(10.0.0.0/8[0]:any)
    Destination(192.168.10.0/24[0]:any)
    Side(Initiator), Status(Established)

[No 0002]
    (Current IPsec SA)
    Mode(tunnel)
    Local-IP(ppp0: [redacted])
    Peer-IP([redacted])
    Direction(OUT), Protocol(ESP), Spi(3347380778,0xc784fa2a)
    Source(192.168.10.0/24[0]:any)
    Destination(10.0.0.0/8[0]:any)
    Side(Initiator), Status(Established)
```


Copyright 2014 FUJITSU LIMITED

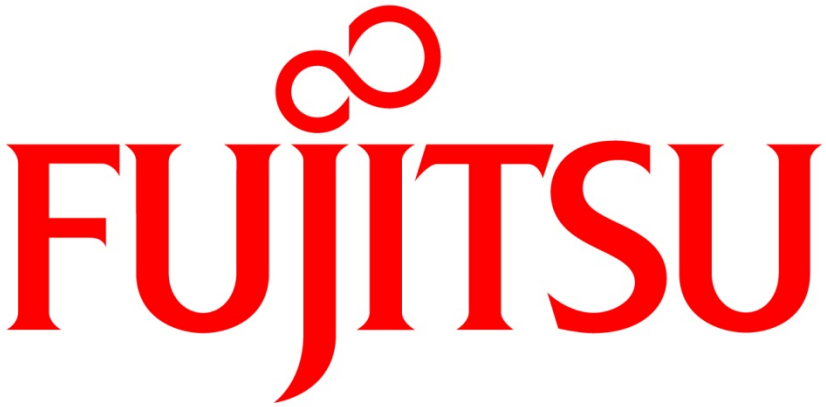
5. 接続が上手くいかない時の確認方法

FUJITSU

- IPsecが接続出来ない時に確認する内容を紹介します。
  - IPsecのトラブルシュートには以下のコマンドが利用出来ます。まずは定義上の問題が無いかを確認して、次にメッセージログの確認を行って下さい。

コマンド名	確認出来る内容
show logging message	IKE,IPsecの接続に関する成功、失敗等をメッセージログとして確認する事が出来ます。ログ内容の詳細は「保守ガイド」に記載されています。
show ike summary	IKEの確立に関する統計情報が確認出来ます。detail等の引数で詳細情報を出す事も可能です。
show ipsec-information summary	IPsecトンネルの確立に関する統計情報が確認出来ます。detail等の引数で詳細情報を出す事も可能です。
trace-network intefaceXX ↓(キャプチャー時間) save trace-network interfaceXX ↓ no trace-network interfaceXX	指定したInterface上に流れるパケットをキャプチャする事が出来ます。生成したpcapファイルは、wireshark等のツールで確認する事が出来ます。必要な期間だけキャプチャし、確認終了後は必ず(no trace-network コマンドで)止めて下さい。

Copyright 2014 FUJITSU LIMITED



shaping tomorrow with you