Juniper SRXとMicrosoft Azure仮想ネットワークとのサイト間VPN接続の構成

Juniper Networks K.K.

2015年3月

はじめに

本資料では、日本マイクロソフト様Microsoft　Azureクラウドサービスにおける仮想ネットワークのゲートウェイ機能と、オンプレミスサイトとのサイト間IPsec　VPN接続について、オンプレミス側VPN機器としてSRXを使用した場合の構成例を説明しています。

本構成例は、ご自身の責任のもとでご利用いただけますようお願いいたします。
また本資料は2015年3月現在の仕様に基いて作成されておりますので、仕様変更等により画面デザインや設定方法が異なる場合がございます。

Microsoft Azure 仮想ネットワークサイト間接続手順

1. 構成ネットワークと設定情報の確認
2. Microsoft Azure 管理ポータルから、Microsoft Azureを構成
   - Microsoft Azure仮想ネットワークの構成
   - ローカルネットワークの構成
   - 共有キーとゲートウェイIPアドレスの確認
3. SRXの構成
   - SRX設定サンプルコンフィグ入手（オプション）
   - SRXのバージョン確認
   - SRXの設定
4. 接続と確認
   - Microsoft Azure仮想ネットワーク側
   - SRX側
5. 接続できない時
   - 状態確認
   - デバッグ

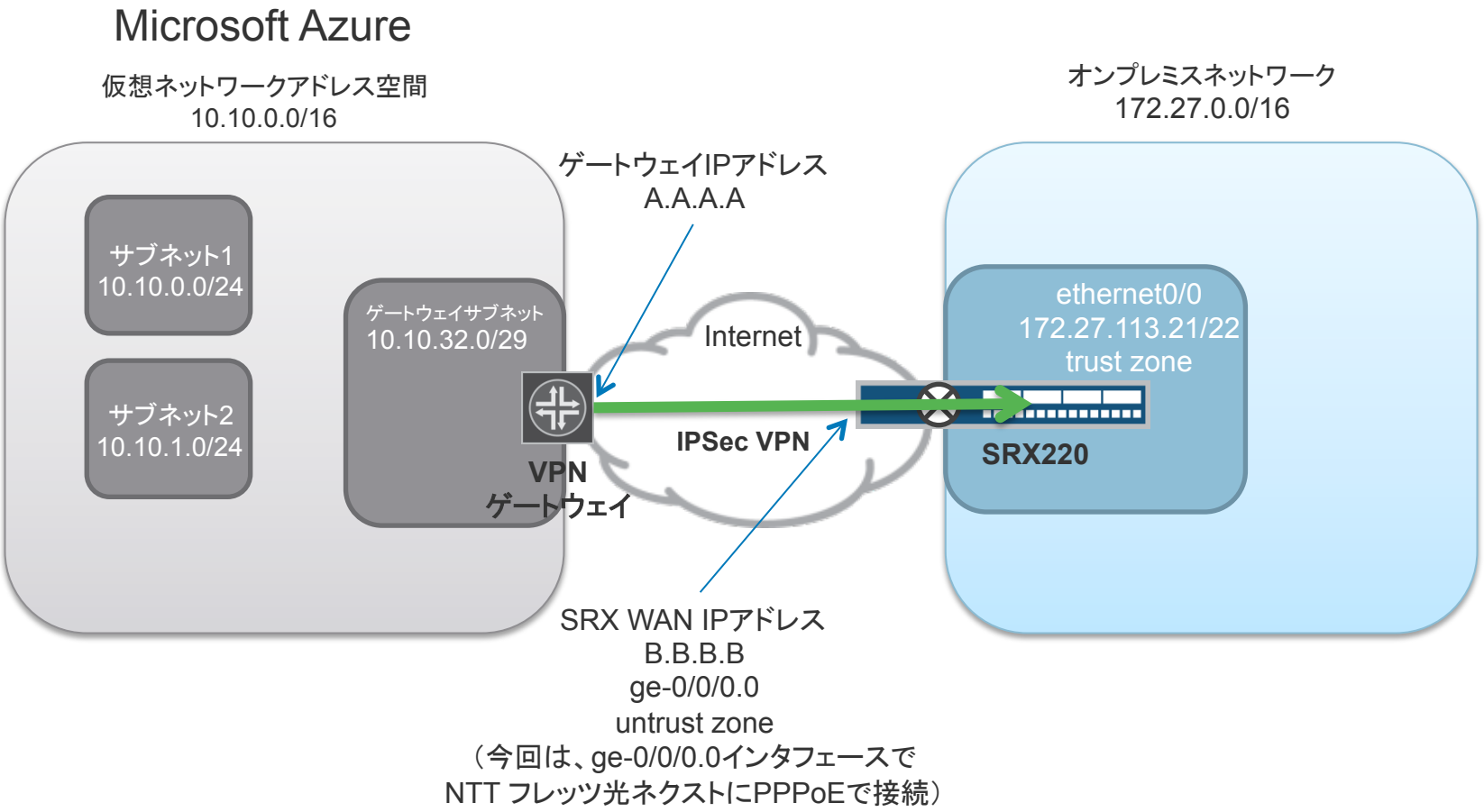
1. 構成ネットワークと設定情報の確認
VPNデバイスとネットワーク環境要件

Microsoft Azure仮想ネットワークとの接続には、グローバルなIPv4アドレスおよび互換性のあるVPN機器が必要です。

詳細な仕様については下記を参照して下さい。
https://msdn.microsoft.com/ja-jp/library/azure/jj156075.aspx

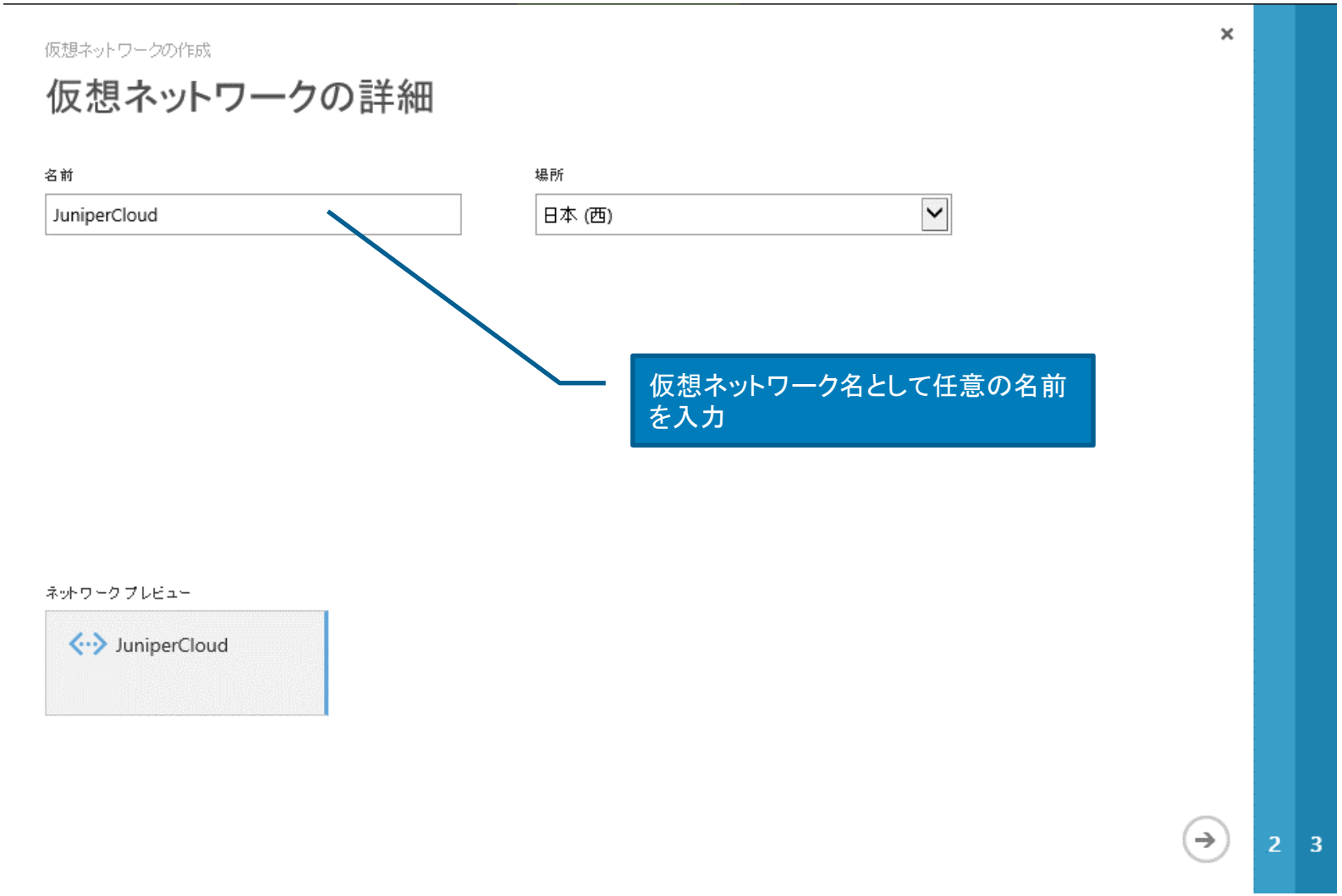
SRXおよびNS/SRXは上記要件を満たしています。(SRXの仮想アプライアンスvSRXも含む)

1. 構成ネットワークと設定情報の確認
構成ネットワーク例

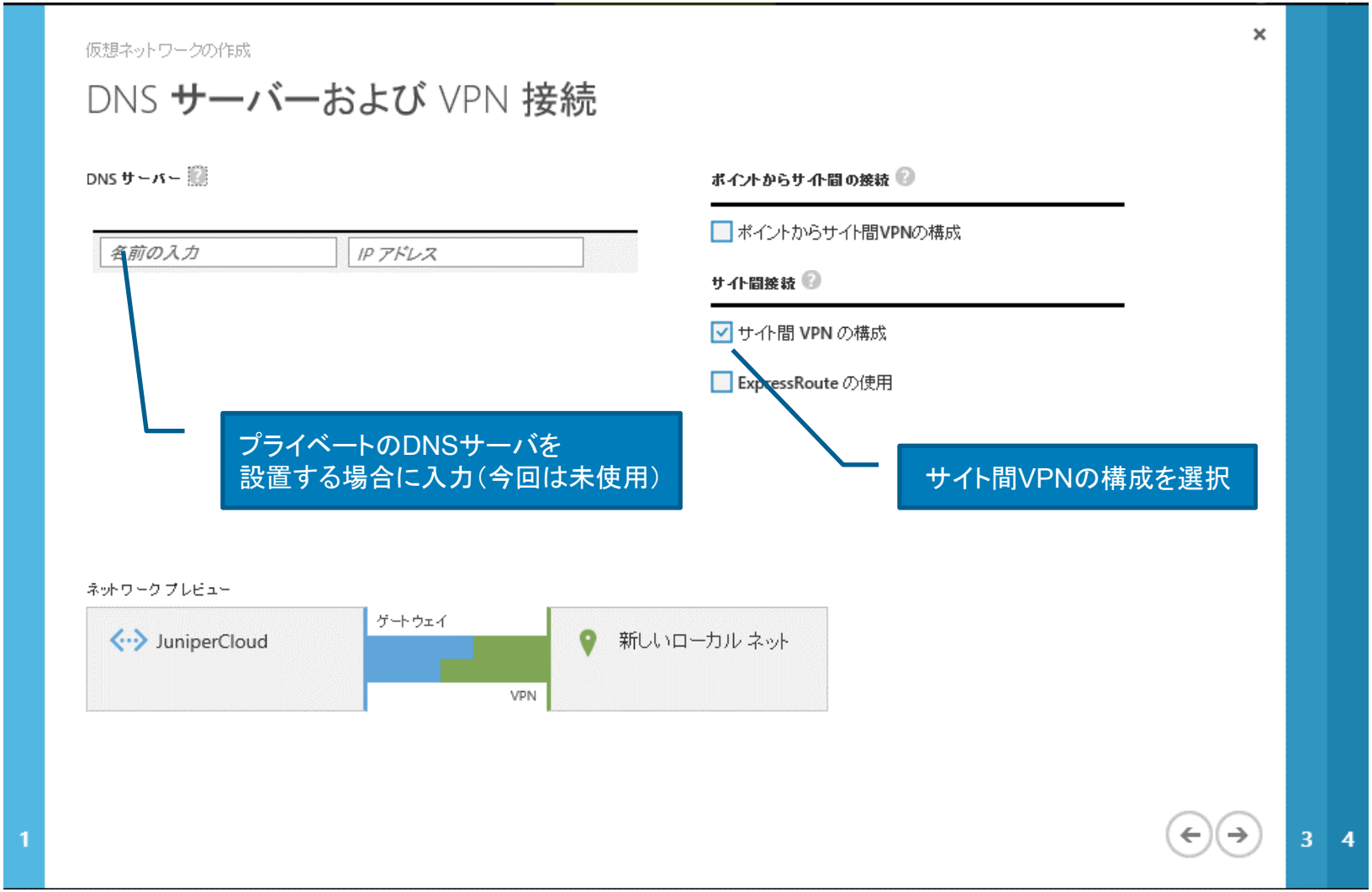


2. Microsoft Azureの構成例

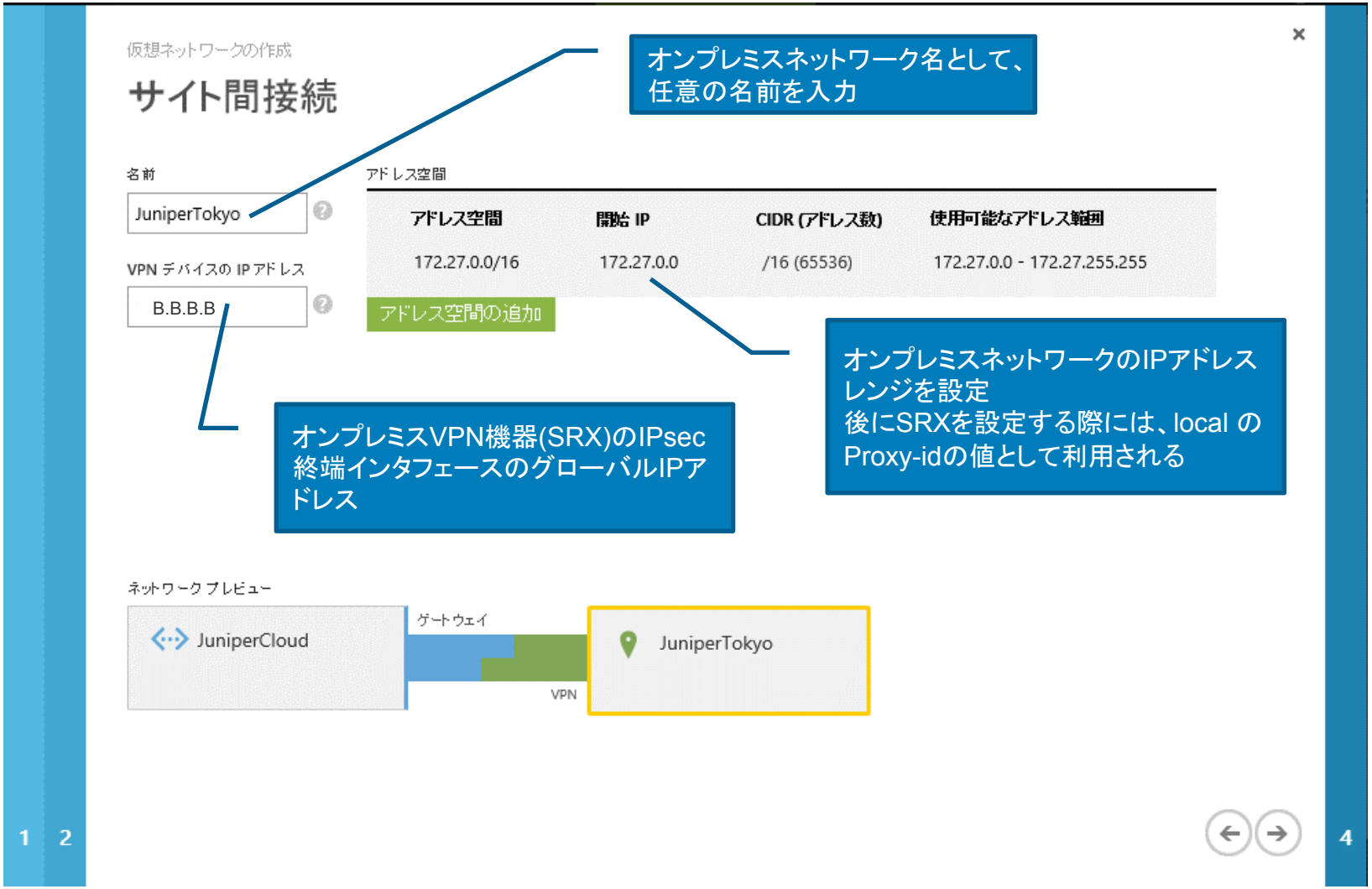
2. Microsoft Azureの構成例
仮想ネットワークの構成①



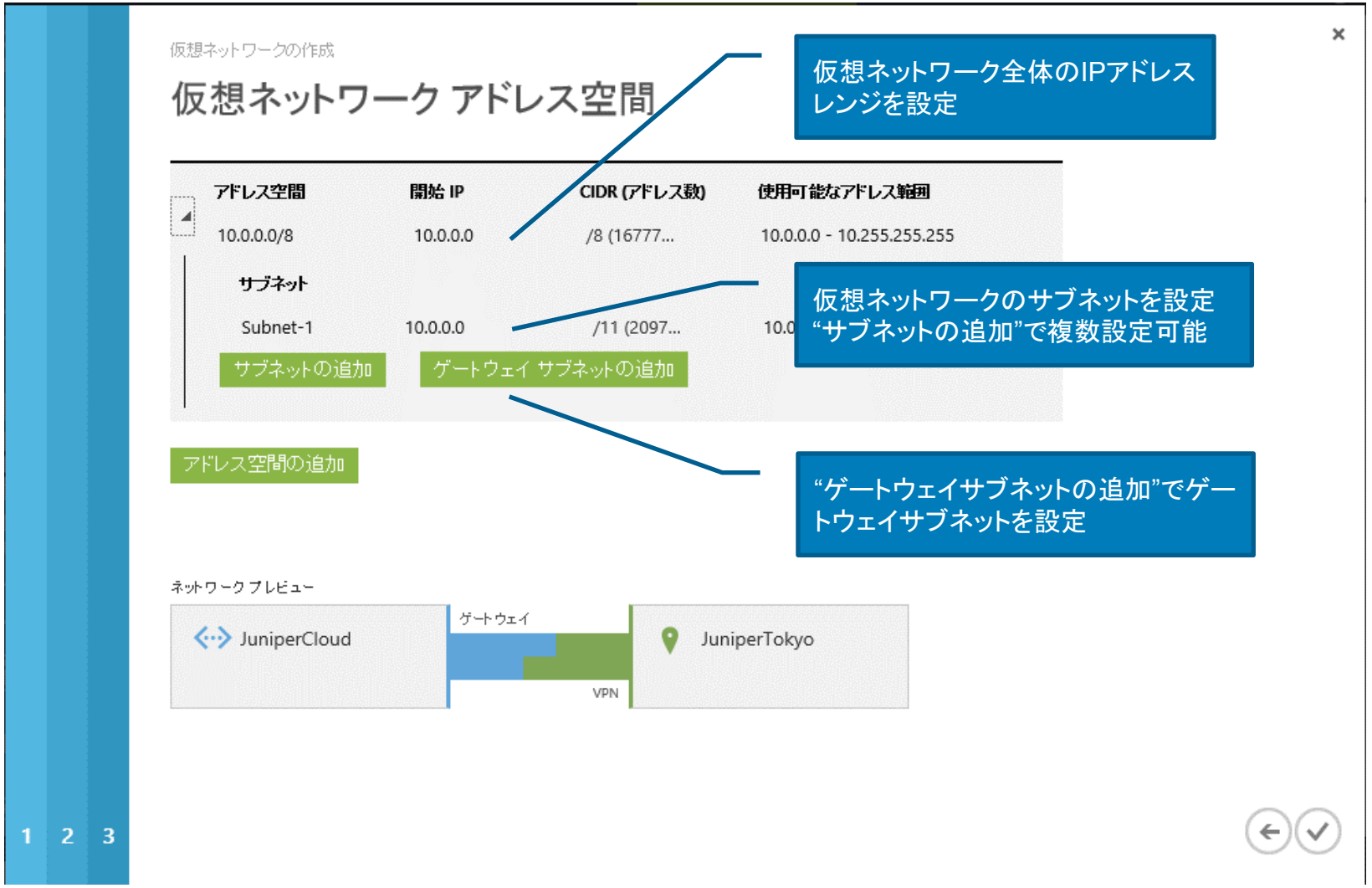
2. Microsoft Azureの構成例
仮想ネットワークの構成②



2. Microsoft Azureの構成例
オンプレミスネットワークの構成

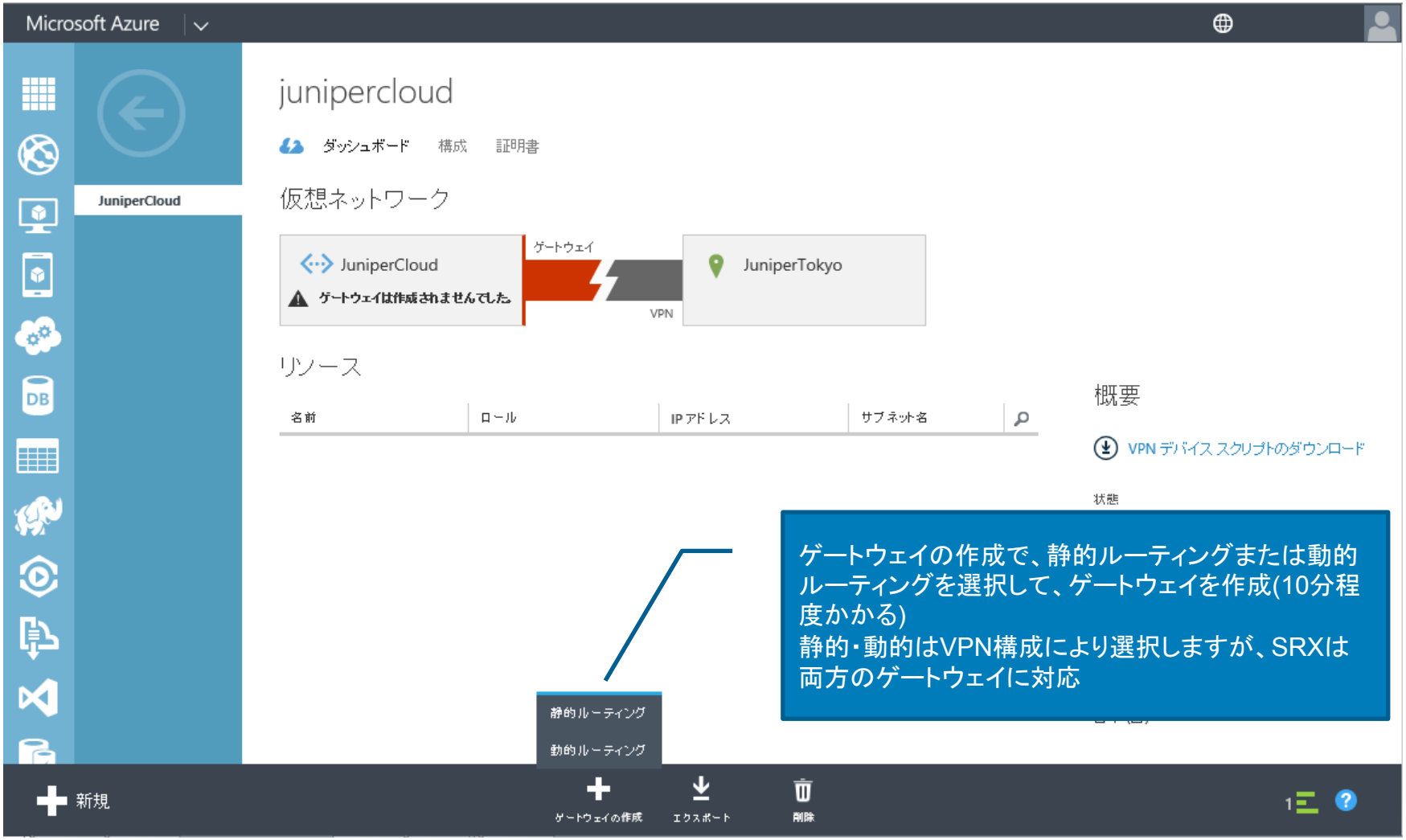


2. Microsoft Azureの構成例
仮想ネットワークの構成③

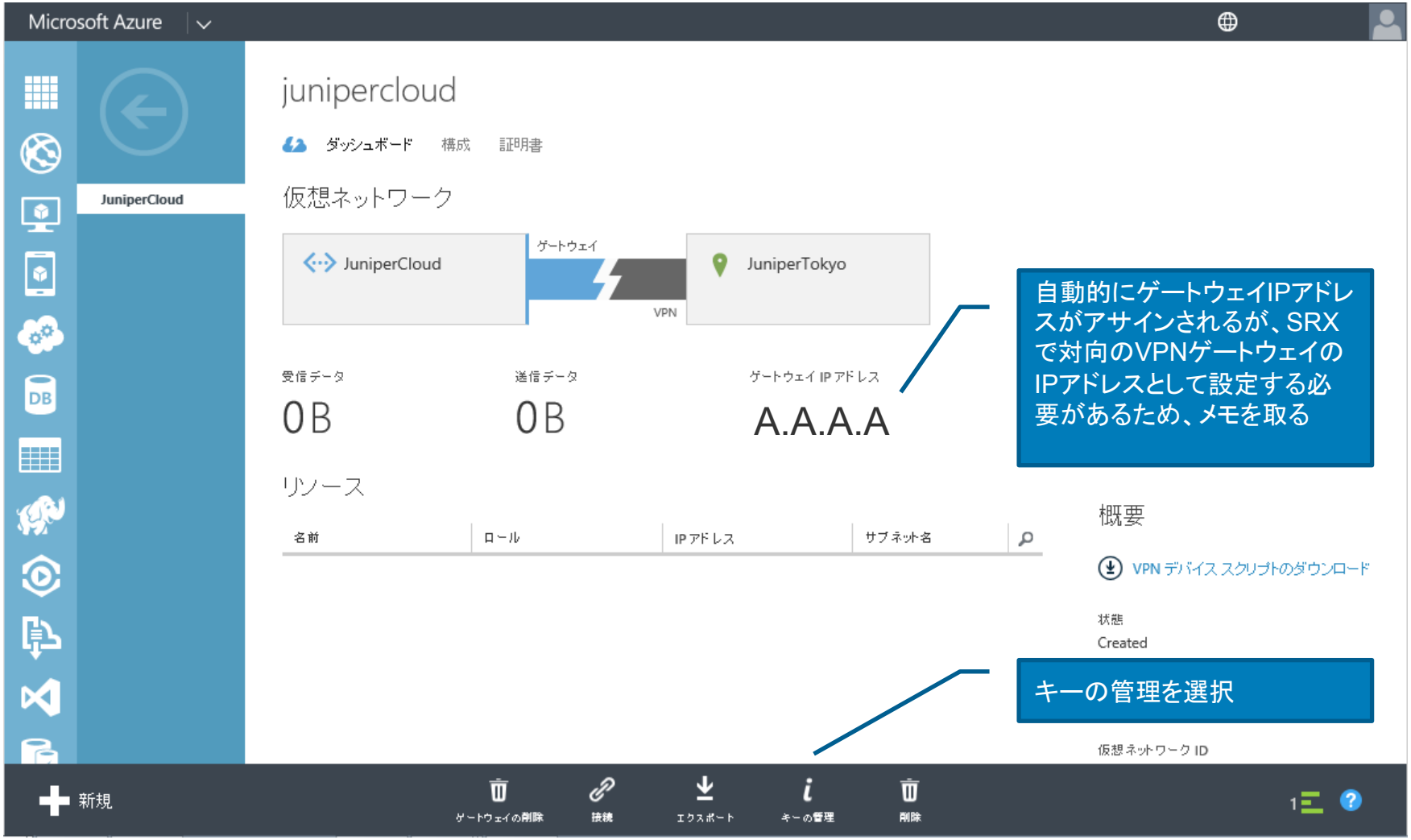


2. Microsoft Azureの構成例
ゲートウェイの作成①

2. Microsoft Azureの構成例
ゲートウェイの作成②



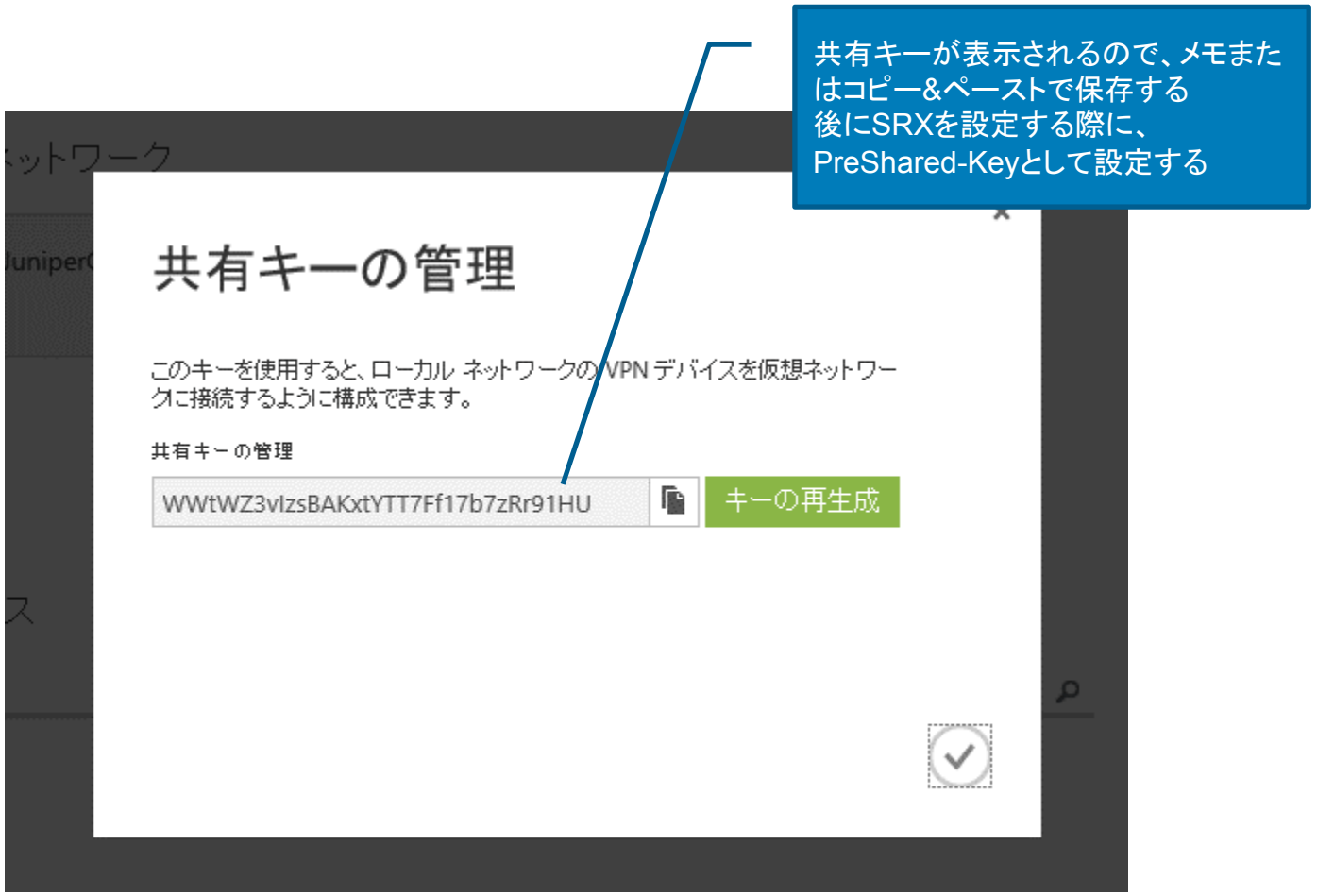
2. Microsoft Azureの構成例
共有キーとゲートウェイIPアドレスの確認①



自動的にゲートウェイIPアドレスがアサインされるが、SRXで対向のVPNゲートウェイのIPアドレスとして設定する必要があるため、メモを取る

キーの管理を選択

2. Microsoft Azureの構成例
共有キーとゲートウェイIPアドレスの確認②



3. SRXの設定例
本資料での環境と注意事項

SRX220を使用

- 本資料ではSRX220を前提にインタフェース等の設定を行っており、ご使用されるSRXの機種とはインタフェースの割り当てが異なる場合、読み替えて設定を行って下さい。

アクセス回線としてフレッツ光ネクストを使用

- 検証目的のため、本資料では動的IP割り当てのサービスを使用。
  Microsoft AzureのゲートウェイからVPN接続が行われることもあるため、固定IPアドレスの使用を推奨。

JUNOS 12.3X48-D10を使用

- Microsoft Azureの既知のVPNデバイスとしてJUNOS 10.2(静的)および11.4(動的)以上で対応。
  vSRXはJUNOS 12.1X47-D20で動作確認済み。

Microsoft Azure仮想ネットワークVPNゲートウェイの種類

- Microsoft Azure仮想ネットワークのVPNゲートウェイは静的または動的ゲートウェイを選択可能であり、IPsecの要件が異なるため、SRX側もそれぞれのゲートウェイの合わせた設定が必要。
  またポリシーベース、ルートベースVPN構成によってもSRX側の設定が異なる。
  本資料では ルートベース ポリシーベース のラベルで区別。
  動的ゲートウェイは現状ルートベースのVPN構成のみをサポート。

静的ルーティングVPNゲートウェイ使用時の設定

3. SRXの設定例
① インタフェース設定

ルートベース

```
set interfaces ge-0/0/6 unit 0 family inet address 172.27.113.21/22
```

SRX LAN側インタフェース設定

```
set interfaces ge-0/0/0 unit 0 encapsulation ppp-over-ether
set interfaces pp0 unit 1 ppp-options pap default-password "xxxxxxxxxxxxxxx"
set interfaces pp0 unit 1 ppp-options pap local-name "xxxxxxxx@ocn.ne.jp"
set interfaces pp0 unit 1 ppp-options pap local-password "xxxxxxxxxxxxx"
set interfaces pp0 unit 1 ppp-options pap passive
set interfaces pp0 unit 1 pppoe-options underlying-interface ge-0/0/0.0
set interfaces pp0 unit 1 pppoe-options auto-reconnect 10
set interfaces pp0 unit 1 pppoe-options client
set interfaces pp0 unit 1 family inet negotiate-address
```

NTT フレッツ光ネクストのPPPoE接続設定。接続インタフェースはge-0/0/0.0

```
set interfaces st0 unit 0 family inet
```

IPsecトンネルインタフェースである、st0.0インタフェースを作成

3. SRXの設定例
① インタフェース設定

ポリシーベース

```
set interfaces ge-0/0/6 unit 0 family inet address 172.27.113.21/22
```

SRX LAN側インタフェース設定

```
set interfaces ge-0/0/0 unit 0 encapsulation ppp-over-ether
set interfaces pp0 unit 1 ppp-options pap default-password "xxxxxxxxxxxxxxx"
set interfaces pp0 unit 1 ppp-options pap local-name "xxxxxxxx@ocn.ne.jp"
set interfaces pp0 unit 1 ppp-options pap local-password "xxxxxxxxxxxxx"
set interfaces pp0 unit 1 ppp-options pap passive
set interfaces pp0 unit 1 pppoe-options underlying-interface ge-0/0/0.0
set interfaces pp0 unit 1 pppoe-options auto-reconnect 10
set interfaces pp0 unit 1 pppoe-options client
set interfaces pp0 unit 1 family inet negotiate-address
```

NTT フレッツ光ネクストのPPPoE接続設定。接続インタフェースは、ge-0/0/0.0

3. SRXの設定例
② ルーティング設定

ルートベース

```
set routing-options static route 172.27.0.0/16 next-hop 172.27.112.1
```

オンプレミスネットワークのルート設定

```
set routing-options static route 0.0.0.0/0 next-hop pp0.1
```

PPPoEインタフェースをデフォルトルートとして設定

```
set routing-options static route 10.10.0.0/16 next-hop st0.0
```

Microsoft Azure仮想ネットワークのアドレス空間のルートとして、IPsecトンネルインタフェースを設定

3. SRXの設定例
② ルーティング設定

ポリシーベース

```
set routing-options static route 172.27.0.0/16 next-hop 172.27.112.1
```

オンプレミスネットワークのルート設定

```
set routing-options static route 0.0.0.0/0 next-hop pp0.1
```

PPPoEインタフェースをデフォルトルートとして設定

3. SRXの設定例
③ IPsec IKE/Phase1設定

ルートベース

ポリシーベース

```
set security ike proposal p1-proposal authentication-method pre-shared-keys
set security ike proposal p1-proposal authentication-algorithm sha1
set security ike proposal p1-proposal encryption-algorithm aes-256-cbc
set security ike proposal p1-proposal lifetime-seconds 28800
set security ike proposal p1-proposal dh-group group2
set security ike policy ike_policy1 proposals p1-proposal
```

Phase 1 Proposalを設定

```
set security ike policy ike_policy1 mode main
```

メインモード選択

```
set security ike policy ike_policy1 pre-shared-key ascii-text "xxxxxxxxxxxxxxx"
```

Microsoft Azure VPNゲートウェイで表示された共有キー

```
set security ike gateway azure_gw ike-policy ike_policy1
set security ike gateway azure_gw address A.A.A.A
```

Microsoft Azure VPNゲートウェイのIPアドレス

```
set security ike gateway azure_gw external-interface pp0.1
```

IKE確立のインタフェースとしてPPPoEインタフェースを指定

3. SRXの設定例
④IPsec/Phase2設定

ルートベース

```
set security ipsec proposal p2-proposal protocol esp
set security ipsec proposal p2-proposal authentication-algorithm hmac-sha1-96
set security ipsec proposal p2-proposal encryption-algorithm aes-256-cbc
set security ipsec proposal p2-proposal lifetime-seconds 3600
set security ipsec policy p2_policy1 proposals p2-proposal
```

Phase 2 Proposalを設定

```
set security ipsec vpn azure_vpn bind-interface st0.0
```

IPSecトンネルインタフェースを指定

```
set security ipsec vpn azure_vpn ike gateway azure_gw
```

使用するIKE設定を指定

```
set security ipsec vpn azure_vpn ike proxy-identity local 172.27.0.0/16
```

Localのproxy-idとして、オンプレミスネットワークのサブネットを指定

```
set security ipsec vpn azure_vpn ike proxy-identity remote 10.10.0.0/16
```

Remoteのproxy-idとして、Microsoft Azure仮想ネットワークのアドレス空間を指定

```
set security ipsec vpn azure_vpn ike proxy-identity service any
set security ipsec vpn azure_vpn ike ipsec-policy p2_policy1
set security flow tcp-mss ipsec-vpn mss 1320
```

TCPのMSSを1320に設定。（通常は1350で良いが、PPPoE接続の為これより小さい値）

3. SRXの設定例
④IPsec/Phase2設定

ポリシーベース

```
set security ipsec proposal p2-proposal protocol esp
set security ipsec proposal p2-proposal authentication-algorithm hmac-sha1-96
set security ipsec proposal p2-proposal encryption-algorithm aes-256-cbc
set security ipsec proposal p2-proposal lifetime-seconds 3600
set security ipsec policy p2_policy1 proposals p2-proposal
```

Phase 2 Proposalを設定

```
set security ipsec vpn azure_vpn ike gateway azure_gw
```

使用するIKE設定を指定

```
set security ipsec vpn azure_vpn ike ipsec-policy p2_policy1
set security flow tcp-mss ipsec-vpn mss 1320
```

TCPのMSSを1320に設定。（通常は1350で良いが、PPPoE接続の為これより小さい値）

3. SRXの設定例
⑤ゾーン設定

ルートベース

```
set security zones security-zone untrust interfaces ge-0/0/0.0
set security zones security-zone untrust interfaces pp0.1 host-inbound-traffic system-
 services ike
```

PPPoEインタフェースで、IKEのパケットを受信できるように設定

```
set security address-book global address Azure_NW 10.10.0.0/20
set security address-book global address Onpremise_NW 172.27.0.0/16
```

Microsoft Azure 仮想ネットワーク側のアドレス空間とオンプレミスネットワークのネットワークをアドレスブックとして作成

```
set security zones security-zone azure_zone interfaces st0.0
```

Microsoft Azure 仮想ネットワークのセキュリティゾーンazure_zoneにIpsecトンネルインタフェースをバインド

```
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust interfaces ge-0/0/6.0
```

2. SRXの設定例
⑤ゾーン設定

ポリシーベース

```
set security zones security-zone untrust interfaces ge-0/0/0.0
set security zones security-zone untrust interfaces pp0.1 host-inbound-traffic system-
 services ike
```

PPPoEインタフェースで、IKEのパケットを受信できるように設定

```
set security address-book global address Azure_NW 10.10.0.0/20
set security address-book global address Onpremise_NW 172.27.0.0/16
```

Microsoft Azure 仮想ネットワーク側のアドレス空間とオンプレミスネットワークのネットワークをアドレスブックとして作成

```
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust interfaces ge-0/0/6.0
```

3. SRXの設定例 ⑥ポリシー設定

ルートベース

```
set security policies from-zone trust to-zone untrust policy trust-to-untrust match
 source-address any
set security policies from-zone trust to-zone untrust policy trust-to-untrust match
 destination-address any
set security policies from-zone trust to-zone untrust policy trust-to-untrust match
 application any
set security policies from-zone trust to-zone untrust policy trust-to-untrust then permit
```

オンプレミスネットワークからインターネット向けの通信はすべて許可のポリシー

```
set security policies from-zone trust to-zone azure_zone policy trust-to-azure_zone match
 source-address Onpremise_NW
set security policies from-zone trust to-zone azure_zone policy trust-to-azure_zone match
 destination-address Azure_NW
set security policies from-zone trust to-zone azure_zone policy trust-to-azure_zone match
 application any
set security policies from-zone trust to-zone azure_zone policy trust-to-azure_zone then
 permit
```

オンプレミスネットワークからIPsecトンネルを介したMicrosoft Azure 仮想ネットワークへの通信はすべて許可のポリシー。この時、source-addressはIpsec VPN設定のproxy-id localに、destination-addresはIPsec VPN設定のproxy-id remoteと一致したアドレスブックエントリを使用

3. SRXの設定例
⑥ポリシー設定

ルートベース

```
set security policies from-zone azure_zone to-zone trust policy azure_zone-to-trust match
 source-address Azure_NW
Set security policies from-zone azure_zone to-zone trust policy azure_zone-to-trust match
 destination-address Onpremise_NW
set security policies from-zone azure_zone to-zone trust policy azure_zone-to-trust match
 application any
set security policies from-zone azure_zone to-zone trust policy azure_zone-to-trust then
 permit
```

Microsoft Azure 仮想ネットワークからIPsecトンネルを介したオンプレミスネットワークへの通信はすべて許可のポリシー。このとき、source-addressはIPsec VPN設定のproxy-id remoteに、destination-addressはIPsec VPN設定のproxy-id localと一致したアドレスブックエントリを使用

3. SRXの設定例
⑥ポリシー設定

ポリシーベース

```
set security policies from-zone trust to-zone untrust policy trust-to-untrust match
 source-address any
set security policies from-zone trust to-zone untrust policy trust-to-untrust match
 destination-address any
set security policies from-zone trust to-zone untrust policy trust-to-untrust match
 application any
set security policies from-zone trust to-zone untrust policy trust-to-untrust then permit
```

オンプレミスネットワークからインターネット向けの通信はすべて許可のポリシー

```
set security policies from-zone trust to-zone azure_zone policy trust-to-azure_zone match
 source-address Onpremise_NW
set security policies from-zone trust to-zone azure_zone policy trust-to-azure_zone match
 destination-address Azure_NW
set security policies from-zone trust to-zone azure_zone policy trust-to-azure_zone match
 application any
set security policies from-zone trust to-zone azure_zone policy trust-to-azure_zone then
 permit tunnel ipsec-vpn azure_vpn
set security policies from-zone trust to-zone azure_zone policy trust-to-azure_zone then
 permit tunnel pair-policy azure_zone-to-trust
```

オンプレミスネットワークからMicrosoft Azure 仮想ネットワークへの通信を許可し、VPNで設定したVPN Nameにバインド

3. SRXの設定例
⑥ポリシー設定

ポリシーベース

```
set security policies from-zone azure_zone to-zone trust policy azure_zone-to-trust match
 source-address Azure_NW
Set security policies from-zone azure_zone to-zone trust policy azure_zone-to-trust match
 destination-address Onpremise_NW
set security policies from-zone azure_zone to-zone trust policy azure_zone-to-trust match
 application any
set security policies from-zone azure_zone to-zone trust policy azure_zone-to-trust then
 permit tunnel ipsec-vpn azure_vpn
set security policies from-zone azure_zone to-zone trust policy azure_zone-to-trust then
 permit tunnel pair-policy trust-to-azure_zone
```

Microsoft Azure 仮想ネットワークからオンプレミスネットワークへの通信を許可し、VPNで設定したVPN Nameにバインド

動的ルーティングVPNゲートウェイ使用時の設定

3. SRXの設定例
① インタフェース設定

ルートベース

```
set interfaces ge-0/0/6 unit 0 family inet address 172.27.113.21/22
```

SRX LAN側インタフェース設定

```
set interfaces ge-0/0/0 unit 0 encapsulation ppp-over-ether
set interfaces pp0 unit 1 ppp-options pap default-password "xxxxxxxxxxxxxxx"
set interfaces pp0 unit 1 ppp-options pap local-name "xxxxxxxx@ocn.ne.jp"
set interfaces pp0 unit 1 ppp-options pap local-password "xxxxxxxxxxxxx"
set interfaces pp0 unit 1 ppp-options pap passive
set interfaces pp0 unit 1 pppoe-options underlying-interface ge-0/0/0.0
set interfaces pp0 unit 1 pppoe-options auto-reconnect 10
set interfaces pp0 unit 1 pppoe-options client
set interfaces pp0 unit 1 family inet negotiate-address
```

NTT フレッツ光ネクストのPPPoE接続設定。接続インタフェースは、ge-0/0/0.0

```
set interfaces st0 unit 0 family inet
```

IPsecトンネルインタフェースである、st0.0インタフェースを作成

3. SRXの設定例
② ルーティング設定

ルートベース

```
set routing-options static route 172.27.0.0/16 next-hop 172.27.112.1
```

オンプレミスネットワークのルート設定

```
set routing-options static route 0.0.0.0/0 next-hop pp0.1
```

PPPoEインタフェースをデフォルトルートとして設定

```
set routing-options static route 10.10.0.0/16 next-hop st0.0
```

Microsoft Azure仮想ネットワークのアドレス空間へのルートとして、IPSecトンネルインタフェースを設定

3. SRXの設定例
③ IPsec IKE/Phase1設定

ルートベース

```
set security ike proposal p1-proposal authentication-method pre-shared-keys
set security ike proposal p1-proposal authentication-algorithm sha1
set security ike proposal p1-proposal encryption-algorithm aes-256-cbc
set security ike proposal p1-proposal lifetime-seconds 28800
set security ike proposal p1-proposal dh-group group2
set security ike policy ike_policy1 proposals p1-proposal
```

Phase 1 Proposalを設定

```
set security ike policy ike_policy1 mode main
```

メインモード選択

```
set security ike policy ike_policy1 pre-shared-key ascii-text "xxxxxxxxxxxxxxx"
```

Microsoft Azure VPNゲートウェイで表示された共有キー

```
set security ike gateway azure_gw ike-policy ike_policy1
set security ike gateway version v2-only
set security ike gateway azure_gw address A.A.A.A
```

Microsoft Azure　VPNゲートウェイのIPアドレス

```
set security ike gateway azure_gw external-interface pp0.1
```

IKE確立のインタフェースとしてPPPoEインタフェースを指定

3. SRXの設定例
④IPsec/Phase2設定

ルートベース

```
set security ipsec proposal p2-proposal protocol esp
set security ipsec proposal p2-proposal authentication-algorithm hmac-sha1-96
set security ipsec proposal p2-proposal encryption-algorithm aes-256-cbc
set security ipsec proposal p2-proposal lifetime-seconds 3600
set security ipsec policy p2_policy1 proposals p2-proposal
```

Phase 2 Proposalを設定

```
set security ipsec vpn azure_vpn bind-interface st0.0
```

IPSecトンネルインタフェースを指定

```
set security ipsec vpn azure_vpn ike gateway azure_gw
```

使用するIKE設定を指定

```
set security ipsec vpn azure_vpn ike ipsec-policy p2_policy1
set security flow tcp-mss ipsec-vpn mss 1320
```

TCPのMSSを1320に設定。（通常は1350で良いが、PPPoE接続の為これより小さい値）

3. SRXの設定例
⑤ゾーン設定

ルートベース

```
set security zones security-zone untrust interfaces ge-0/0/0.0
set security zones security-zone untrust interfaces pp0.1 host-inbound-traffic system-
 services ike
```

PPPoEインタフェースで、IKEのパケットを受信できるように設定

```
set security address-book global address Azure_NW 10.10.0.0/20
set security address-book global address Onpremise_NW 172.27.0.0/16
```

Microsoft Azure 仮想ネットワーク側のアドレス空間とオンプレミスネットワークのネットワークをアドレスブックとして作成

```
set security zones security-zone azure_zone interfaces st0.0
```

Microsoft Azure 仮想ネットワークのセキュリティゾーンazure_zoneにIpsecトンネルインタフェースをバインド

```
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust interfaces ge-0/0/6.0
```

3. SRXの設定例
⑥ポリシー設定

ルートベース

```
set security policies from-zone trust to-zone untrust policy trust-to-untrust match
 source-address any
set security policies from-zone trust to-zone untrust policy trust-to-untrust match
 destination-address any
set security policies from-zone trust to-zone untrust policy trust-to-untrust match
 application any
set security policies from-zone trust to-zone untrust policy trust-to-untrust then permit
```

オンプレミスネットワークからインターネット向けの通信はすべて許可のポリシー

```
set security policies from-zone trust to-zone azure_zone policy trust-to-azure_zone match
 source-address Onpremise_NW
set security policies from-zone trust to-zone azure_zone policy trust-to-azure_zone match
 destination-address Azure_NW
set security policies from-zone trust to-zone azure_zone policy trust-to-azure_zone match
 application any
set security policies from-zone trust to-zone azure_zone policy trust-to-azure_zone then
 permit
```

オンプレミスネットワークからIPsecトンネルを介したMicrosoft Azure 仮想ネットワークへの通信はすべて許可のポリシー。

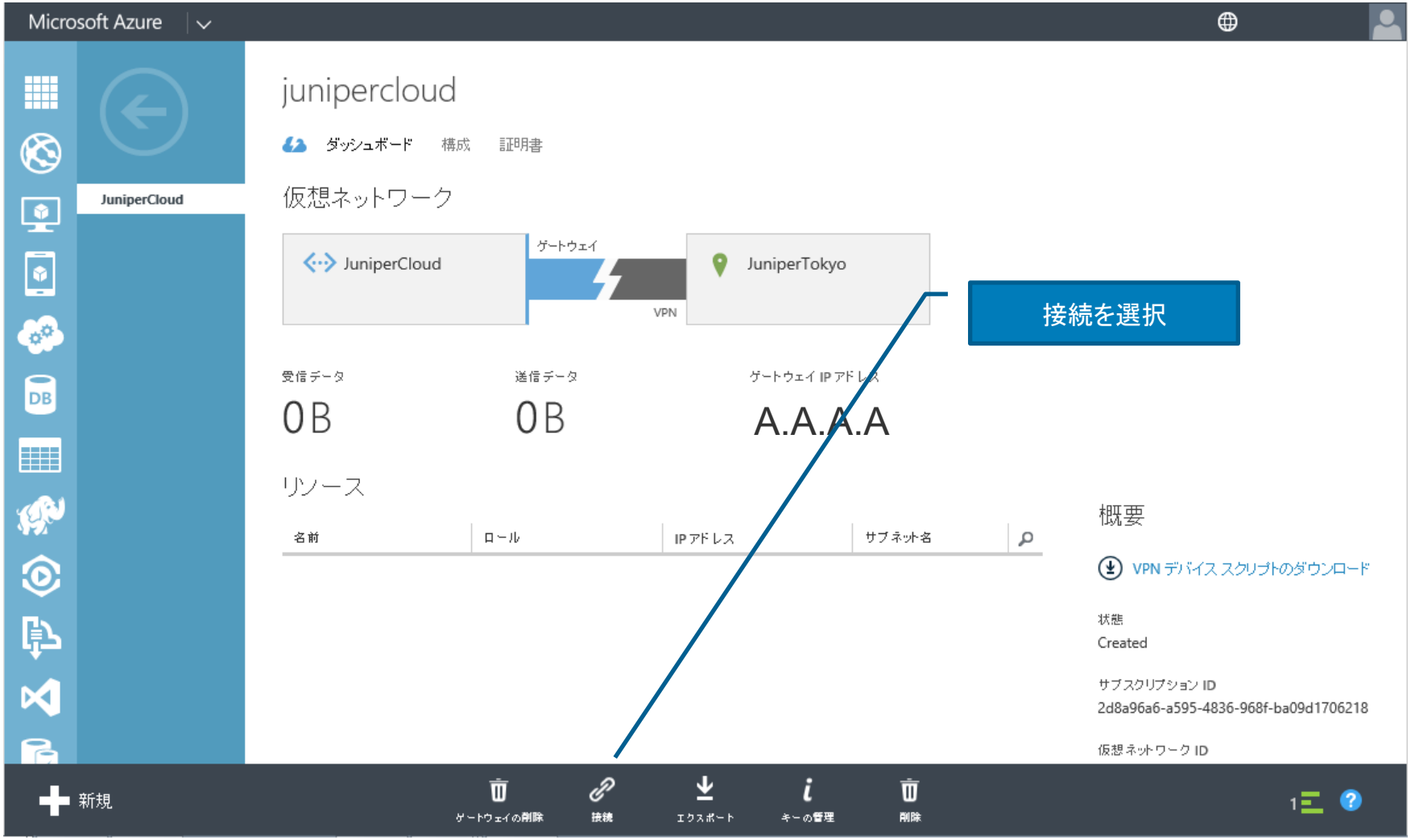
3. SRXの設定例
⑥ポリシー設定

ルートベース

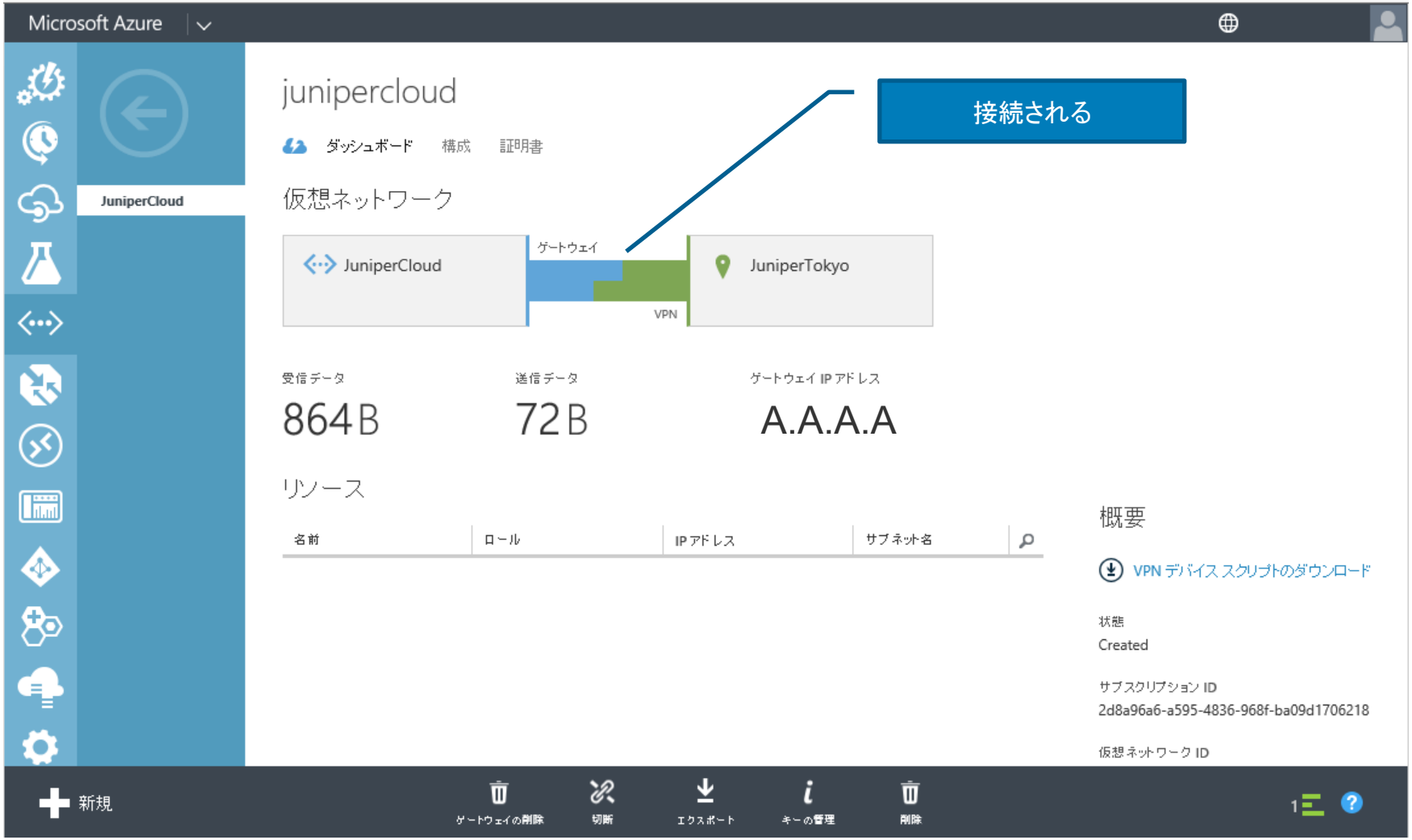
```
set security policies from-zone azure_zone to-zone trust policy azure_zone-to-trust match
 source-address Azure_NW
Set security policies from-zone azure_zone to-zone trust policy azure_zone-to-trust match
 destination-address Onpremise_NW
set security policies from-zone azure_zone to-zone trust policy azure_zone-to-trust match
 application any
set security policies from-zone azure_zone to-zone trust policy azure_zone-to-trust then
 permit
```

Microsoft Azure 仮想ネットワークからIPsecトンネルを介したオンプレミスネットワークへの通信はすべて許可のポリシー。

4. 接続と確認
Microsoft Azureからの接続リクエスト



4. 接続と確認
Microsoft Azure接続確認



5. 接続できない・通信ができない時 よくある問題

Proxy-IDとポリシーオブジェクトの不一致

- IPsec Phase2設定のProxy IDのLocal/Remote IPと該当するセキュリティポリシーのsource-address/destination-addressが一致していないと、Proxy IDのネゴシエーションが失敗します。VPN設定と、ポリシーのこれら値が一致していることを確認してください。

Microsoft Azure管理ポータルのステータス

- Microsoft Azure管理ポータルでは、接続/切断を実行後にもVPNのステータスがすぐには反映されないことがあります。Microsoft Azure管理ポータルでVPNが接続/切断であっても、SRX側で正常に接続/切断されている状態のときは、ステータスが更新されるまでお待ち下さい。

5. 接続と確認
SRX側接続確認: IPsec Phase1接続ステータス

```
root@srx220> show security ike security-associations
Index   State  Initiator cookie  Responder cookie  Mode           Remote Address
4408876 UP     75de10ae18e72dc8  46c1e8c60925bd6e  Main           A.A.A.A
```

StateがUPとなる

```
root@srx220> show security ike security-associations detail
IKE peer A.A.A.A, Index 565956, Gateway Name: azure-gateway
  Role: Responder, State: UP
  Initiator cookie: 3876ef037857f48d, Responder cookie: 1f752bd6a4c59901
  Exchange type: Main, Authentication method: Pre-shared-keys
  Local: B.B.B.B:500, Remote: A.A.A.A:500
  Lifetime: Expires in 28727 seconds
  Peer ike-id: A.A.A.A
  Xauth user-name: not available
  Xauth assigned IP: 0.0.0.0
  Algorithms:
   Authentication        : hmac-sha1-96
   Encryption            : aes256-cbc
   Pseudo random function: hmac-sha1
   Diffie-Hellman group  : DH-group-2
  Traffic statistics:
   Input  bytes  :                 1908
   Output bytes  :                  884
   Input  packets:                    7
   Output packets:                    6
  IPSec security associations: 1 created, 0 deleted
  Phase 2 negotiations in progress: 1
```

詳細接続情報

5. 接続と確認
SRX側接続確認: IPsec Phase2接続ステータス

```
root@srx220> show security ipsec security-associations
  Total active tunnels: 1
  ID    Algorithm       SPI      Life:sec/kb  Mon lsys Port  Gateway
  <131073 ESP:aes-cbc-256/sha1 f6124ca9 3579/ unlim - root 500 A.A.A.A
  >131073 ESP:aes-cbc-256/sha1 3c11e98a 3579/ unlim - root 500 A.A.A.A
```

SAが確立されていることを確認

```
root@iga_srx220> show security ipsec security-associations detail

ID: 131073 Virtual-system: root, VPN Name: azure-vpn
  Local Gateway: B.B.B.B, Remote Gateway: A.A.A.A
  Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
  Remote Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
  Version: IKEv2
  DF-bit: clear, Bind-interface: st0.0
  Port: 500, Nego#: 70, Fail#: 0, Def-Del#: 0 Flag: 0x600a29
  Tunnel events:
    Tue Mar 31 2015 16:49:20
    : IPSec SA negotiation successfully completed          (1 times)
    Tue Mar 31 2015 16:49:20
    : IKE SA negotiation successfully completed            (2 times)
    Tue Mar 31 2015 01:07:31
    : IKE SA rekey successfully completed                  (2 times)
    Mon Mar 30 2015 19:25:31
    : IKE SA negotiation successfully completed            (1 times)
    Mon Mar 30 2015 18:27:01
```

詳細接続情報

5. 接続と確認
SRX側接続確認: セッション確認

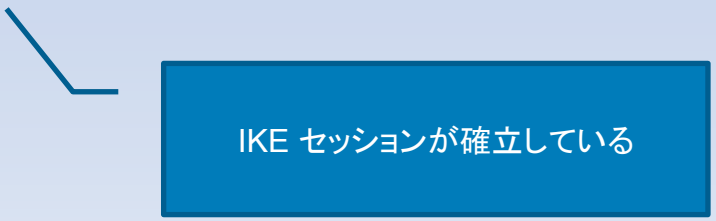
```
root@srx220> show security flow session
Session ID: 11852, Policy name: N/A, Timeout: N/A, Valid
  In: A.A.A.A/46179 --> B.B.B.B/20933;esp, If: pp0.1, Pkts: 0, Bytes: 0

Session ID: 11853, Policy name: N/A, Timeout: N/A, Valid
  In: A.A.A.A/0 --> B.B.B.B/0;esp, If: pp0.1, Pkts: 0, Bytes: 0

Session ID: 14385, Policy name: N/A, Timeout: N/A, Valid
  In: A.A.A.A/30730 --> B.B.B.B/20945;esp, If: pp0.1, Pkts: 0, Bytes: 0

Session ID: 14386, Policy name: N/A, Timeout: N/A, Valid
  In: A.A.A.A/0 --> B.B.B.B/0;esp, If: pp0.1, Pkts: 0, Bytes: 0

Session ID: 14387, Policy name: N/A, Timeout: N/A, Valid
  In: A.A.A.A/1032 --> B.B.B.B/4500;udp, If: pp0.1, Pkts: 0, Bytes: 0
```



5. 接続できない時
SRX側接続確認: SRX JUNOSバージョン

```
root@srx220> show version
Hostname: srx220
Model: srx220h2
JUNOS Software Release [12.3X48-D10.3]
```

SRX JUNOSのバージョン

5. 接続できない時
SRX側接続確認: インタフェース状態確認

```
root@srx220> show interfaces terse | match ?
Possible completions:
  <pattern>            Pattern to match against
root@srx220> show interfaces terse | match pp
pp0                     up    up
pp0.1                   up    up   inet     B.B.B.B
ppd0                    up    up
ppe0                    up    up
```

pppインタフェースがup
upで無い時はPPPoEの接続に問題あり

```
root@srx220> show interfaces terse | match st
st0                     up    up
st0.0                   up    up   inet
```

st0.0インタフェースが使用可能であり、upであることを確認

4. 接続できない時
SRX側接続確認: ルーティング確認

```
root@srx220> show route

inet.0: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

0.0.0.0/0          *[Static/5] 06:19:12
                    > via pp0.1
10.10.0.0/16       *[Static/5] 04:45:51
                    > via st0.0
172.27.0.0/16      *[Static/5] 06:19:19
                    > to 172.27.112.1 via ge-0/0/6.0
172.27.112.0/22    *[Direct/0] 06:19:19
                    > via ge-0/0/6.0
172.27.113.21/32   *[Local/0] 06:19:23
                       Local via ge-0/0/6.0
B.B.B.B/32         *[Local/0] 06:19:12
                       Local via pp0.1
```

デフォルトルートがpppインタフェースとなっており、up(*マーク)していることを確認

Microsoft Azure仮想ネットワークのルートはst0.0経由となっており、同様にupしていることを確認

5. 接続できない時 SRXでのデバッグ

```
set security ike traceoptions file ike_debug.log
set security ike traceoptions flag all
```

本設定を入れることにより、IPsec VPNのより詳細なデバッグ情報を取得可能

デバッグログファイルの中身を確認して、どのようなエラーが出ているか確認

```
root@srx220> show log ike_debug.log
[Mar  1 15:10:43]ike_get_sa: Start, SA = { f59b44a0 9d324a0b - 00000000 00000000 } /
 00000000, remote = A.A.A.A:500
[Mar  1 15:10:43]ike_sa_allocate: Start, SA = { f59b44a0 9d324a0b - 18410627 b3848da1 }
[Mar  1 15:10:43]ike_init_isakmp_sa: Start, remote = A.A.A.A:500, initiator = 0
[Mar  1 15:10:43]ike_decode_packet: Start
[Mar  1 15:10:43]ike_decode_packet: Start, SA = { f59b44a0 9d324a0b - cab69aaa
 ef773b06} / 00000000, nego = -1
[Mar  1 15:10:43]ike_decode_payload_sa: Start
[Mar  1 15:10:43]ike_decode_payload_t: Start, # trans = 4

<< 省略 >>
```

5. 接続できない時
接続成功時のデバッグ出力例(1)

```
[Mar  1 15:10:43]ike_get_sa: Start, SA = { f59b44a0 9d324a0b - 00000000 00000000 } / 00000000, remote =
 A.A.A.A:500
[Mar  1 15:10:43]ike_sa_allocate: Start, SA = { f59b44a0 9d324a0b - 18410627 b3848d
[Mar  1 15:10:43]ike_init_isakmp_sa: Start, remote = A.A.A.A:500, initiator = 0
[Mar  1 15:10:43]ike_decode_packet: Start
[Mar  1 15:10:43]ike_decode_packet: Start, SA = { f59b44a0 9d324a0b - cab69aaa ef773b06} / 00000000, nego
 = -1
[Mar  1 15:10:43]ike_decode_payload_sa: Start
[Mar  1 15:10:43]ike_decode_payload_t: Start, # trans = 4
[Mar  1 15:10:43]ike_st_i_vid: VID[0..20] = 01528bbb c0069612 ...
[Mar  1 15:10:43]ike_st_i_vid: VID[0..20] = 1e2b5169 05991c7d ...
[Mar  1 15:10:43]ike_st_i_vid: VID[0..16] = 4a131c81 07035845 ...
[Mar  1 15:10:43]ike_st_i_vid: VID[0..16] = 90cb8091 3ebb696e ...
[Mar  1 15:10:43]ike_st_i_vid: VID[0..16] = 4048b7d5 6ebce885 ...
[Mar  1 15:10:43]ike_st_i_vid: VID[0..16] = fb1de3cd f341b7ea ...
[Mar  1 15:10:43]ike_st_i_vid: VID[0..16] = 26244d38 eddb61b3 ...
[Mar  1 15:10:43]ike_st_i_vid: VID[0..16] = e3a5966a 76379fe7 ...
[Mar  1 15:10:43]ike_st_i_sa_proposal: Start
[Mar  1 15:10:43]Peer's proposed IKE SA payload is SA()
[Mar  1 15:10:43]Configured proposal is SA()
[Mar  1 15:10:43]ike_isakmp_sa_reply: Start
[Mar  1 15:10:43]ike_state_restart_packet: Start, restart packet SA = { f59b44a0 9d324a0b - cab69aaa
 ef773b06}, nego = -1
[Mar  1 15:10:43]ike_st_i_sa_proposal: Start
[Mar  1 15:10:43]ike_st_i_cr: Start
[Mar  1 15:10:43]ike_st_i_cert: Start
[Mar  1 15:10:43]ike_st_i_private: Start
[Mar  1 15:10:43]ike_st_o_sa_values: Start
[Mar  1 15:10:43]ike_policy_reply_isakmp_vendor_ids: Start
[Mar  1 15:10:43]ike_st_o_private: Start
[Mar  1 15:10:43]ike_policy_reply_private_payload_out: Start
```

Microsoft Azure 仮想ネットワークからSRXへのIKE message

5. 接続できない時
接続成功時のデバッグ出力例(2)

```
[Mar  1 15:10:43]ike_encode_packet: Start, SA = { 0xf59b44a0 9d324a0b - cab69aaa ef773b06 } / 00000000,
 nego = -1
[Mar  1 15:10:43]ike_send_packet: Start, send SA = { f59b44a0 9d324a0b - cab69aaa ef773b06}, nego = -1,
 dst = A.A.A.A:500,  routing table id = 0
[Mar  1 15:10:43]ikev2_packet_allocate: Allocated packet 102a800 from freelist
[Mar  1 15:10:43]ike_sa_find: Found SA = { f59b44a0 9d324a0b - cab69aaa ef773b06 }
[Mar  1 15:10:43]ikev2_packet_v1_start: Passing IKE v1.0 packet to IKEv1 library
[Mar  1 15:10:43]ike_get_sa: Start, SA = { f59b44a0 9d324a0b - cab69aaa ef773b06 } / 00000000, remote =
 A.A.A.A:500
[Mar  1 15:10:43]ike_sa_find: Found SA = { f59b44a0 9d324a0b - cab69aaa ef773b06 }
[Mar  1 15:10:43]ike_decode_packet: Start
[Mar  1 15:10:43]ike_decode_packet: Start, SA = { f59b44a0 9d324a0b - cab69aaa ef773b06} / 00000000, nego
 = -1
[Mar  1 15:10:43]ike_st_i_nonce: Start, nonce[0..48] = 4ae8968e 46525676 ...
[Mar  1 15:10:43]ike_st_i_ke: Ke[0..128] = 08fe3e00 bbe15281 ...
[Mar  1 15:10:43]ike_st_i_cr: Start
[Mar  1 15:10:43]ike_st_i_cert: Start
[Mar  1 15:10:43]ike_st_i_private: Start
[Mar  1 15:10:43]ike_st_o_ke: Start
[Mar  1 15:10:43]ike_st_o_nonce: Start
[Mar  1 15:10:43]ike_policy_reply_isakmp_nonce_data_len: Start
[Mar  1 15:10:43]ike_find_pre_shared_key: Find pre shared key key for B.B.B.B:500, id = No Id -> A.A.A.A:
 500, id = No Id
[Mar  1 15:10:43]ike_policy_reply_find_pre_shared_key: Start
[Mar  1 15:10:43]ike_state_restart_packet: Start, restart packet SA = { f59b44a0 9d324a0b - cab69aaa
 ef773b06}, nego = -1
[Mar  1 15:10:43]ike_find_pre_shared_key: Find pre shared key key for B.B.B.B:500, id = No Id -> A.A.A.A:
 500, id = No Id
[Mar  1 15:10:43]ike_st_o_private: Start
[Mar  1 15:10:43]ike_st_o_calc_skeyid: Calculating skeyid
[Mar  1 15:10:43]ike_find_pre_shared_key: Find pre shared key key for B.B.B.B:500, id = No Id -> A.A.A.A:
 500, id = No Id
```

Pre-shared-keyの確認

5. 接続できない時
接続成功時のデバッグ出力例(3)

```
[Mar  1 15:10:43]ike_encode_packet: Start, SA = { 0xf59b44a0 9d324a0b - cab69aaa ef773b06 } / 00000000,
 nego = -1
[Mar  1 15:10:43]ike_send_packet: Start, send SA = { f59b44a0 9d324a0b - cab69aaa ef773b06}, nego = -1,
 dst = A.A.A.A:500,  routing table id = 0
[Mar  1 15:10:43]ikev2_packet_allocate: Allocated packet 102ac00 from freelist
[Mar  1 15:10:43]ike_sa_find: Found SA = { f59b44a0 9d324a0b - cab69aaa ef773b06 }
[Mar  1 15:10:43]ikev2_packet_v1_start: Passing IKE v1.0 packet to IKEv1 library
[Mar  1 15:10:43]ike_get_sa: Start, SA = { f59b44a0 9d324a0b - cab69aaa ef773b06 } / 00000000, remote =
 A.A.A.A:500
[Mar  1 15:10:43]ike_sa_find: Found SA = { f59b44a0 9d324a0b - cab69aaa ef773b06 }
[Mar  1 15:10:43]ike_decode_packet: Start
[Mar  1 15:10:43]ike_decode_packet: Start, SA = { f59b44a0 9d324a0b - cab69aaa ef773b06} / 00000000, nego
 = -1
[Mar  1 15:10:43]ike_st_i_encrypt: Check that packet was encrypted succeeded
[Mar  1 15:10:43]ike_st_i_id: Start
[Mar  1 15:10:43]ike_st_i_hash: Start, hash[0..20] = fa8c05a8 60eeb654 ...
[Mar  1 15:10:43]ike_calc_mac: Start, initiator = false, local = false
[Mar  1 15:10:43]ike_st_i_cert: Start
[Mar  1 15:10:43]ike_st_i_private: Start
[Mar  1 15:10:43]ike_st_o_id: Start
[Mar  1 15:10:43]ike_policy_reply_isakmp_id: Start
[Mar  1 15:10:43]ike_state_restart_packet: Start, restart packet SA = { f59b44a0 9d324a0b - cab69aaa
 ef773b06}, nego = -1
[Mar  1 15:10:43]ike_st_o_id: Start
[Mar  1 15:10:43]ike_st_o_hash: Start
[Mar  1 15:10:43]ike_calc_mac: Start, initiator = false, local = true
[Mar  1 15:10:43]ike_st_o_status_n: Start
[Mar  1 15:10:43]ike_st_o_private: Start
[Mar  1 15:10:43]ike_policy_reply_private_payload_out: Start
[Mar  1 15:10:43]ike_st_o_encrypt: Marking encryption for packet
[Mar  1 15:10:43]ike_st_o_wait_done: Marking for waiting for done
```

5. 接続できない時
接続成功時のデバッグ出力例(4)

```
[Mar  1 15:10:43]ike_st_o_all_done: MESSAGE: Phase 1 { 0xf59b44a0 9d324a0b - 0xcab69aaa ef773b06 } /
 00000000, version = 1.0, xchg = Identity protect, auth_method = Pre shared keys, Responder, cipher = aes-
 cbc, hash = sha1, prf = hmac-sha1,
[Mar  1 15:10:43]B.B.B.B:500 (Responder) <-> A.A.A.A:500 { f59b44a0 9d324a0b - cab69aaa ef773b06 [-1] /
 0x00000000 } IP; MESSAGE: Phase 1 version = 1.0, auth_method = Pre shared keys, cipher = aes-cbc, hash =
 sha1, prf = hmac-
[Mar  1 15:10:43]ike_encode_packet: Start, SA = { 0xf59b44a0 9d324a0b - cab69aaa ef773b06 } / 00000000,
 nego = -1
[Mar  1 15:10:43]ike_send_packet: Start, send SA = { f59b44a0 9d324a0b - cab
 dst = A.A.A.A:500,  routing table id = 0
[Mar  1 15:10:43]ike_send_notify: Connected, SA = { f59b44a0 9d324a0b - cab69aaa ef773b06}, nego = -1
[Mar  1 15:10:43]iked_pm_ike_sa_done: local:B.B.B.B, remote:A.A.A.A IKEv1
[Mar  1 15:10:43]IKE negotiation done for local:B.B.B.B, remote:A.A.A.A IKEv1 with status: Error ok
[Mar  1 15:10:43]ikev2_packet_allocate: Allocated packet 102b000 from freelist
[Mar  1 15:10:43]ike_sa_find: Found SA = { f59b44a0 9d324a0b - cab69aaa ef773b06 }
[Mar  1 15:10:43]ikev2_packet_v1_start: Passing IKE v1.0 packet to IKEv1 library
[Mar  1 15:10:43]ike_get_sa: Start, SA = { f59b44a0 9d324a0b - cab69aaa ef773b06 } / 00000001, remote =
 A.A.A.A:500
[Mar  1 15:10:43]ike_sa_find: Found SA = { f59b44a0 9d324a0b - cab69aaa ef773b06 }
[Mar  1 15:10:43]ike_st_o_done: ISAKMP SA negotiation done
[Mar  1 15:10:43]ike_send_notify: Connected, SA = { f59b44a0 9d324a0b - cab69aaa ef773b06}, nego = -1
[Mar  1 15:10:43]ike_free_negotiation_isakmp: Start, nego = -1
[Mar  1 15:10:43]ike_free_negotiation: Start, nego = -1
[Mar  1 15:10:43]ike_alloc_negotiation: Start, SA = { f59b44a0 9d324a0b - cab69aaa ef773b06}
[Mar  1 15:10:43]ike_init_qm_negotiation: Start, initiator = 0, message_id = 00000001
[Mar  1 15:10:43]ike_decode_packet: Start
[Mar  1 15:10:43]ike_decode_packet: Start, SA = { f59b44a0 9d324a0b - cab69aaa ef773b06} / 00000001, nego
 = 0
[Mar  1 15:10:43]ike_decode_payload_sa: Start
[Mar  1 15:10:43]ike_decode_payload_t: Start, # trans = 1
[Mar  1 15:10:43]ike_st_i_encrypt: Check that packet was encrypted succeeded
[Mar  1 15:10:43]ike_st_i_qm_hash_1: Start, hash[0..20] = 0e020a5e 1a0cbe78 ...
```

Phase1の確立

5. 接続できない時
接続成功時のデバッグ出力例(5)

```
[Mar  1 15:10:43]ike_get_sa: Start, SA = { f59b44a0 9d324a0b - cab69aaa ef773b06 } / 00000001, remote =
 A.A.A.A:500
[Mar  1 15:10:43]ike_sa_find: Found SA = { f59b44a0 9d324a0b - cab69aaa ef773b06 }
[Mar  1 15:10:43]ike_decode_packet: Start
[Mar  1 15:10:43]ike_decode_packet: Start, SA = { f59b44a0 9d324a0b - cab69aaa ef773b06} / 00000001, nego
 = 0
[Mar  1 15:10:43]ike_st_i_encrypt: Check that packet was encrypted succeeded
[Mar  1 15:10:43]ike_st_i_qm_hash_3: Start, hash[0..20] = 65cb3fe2 1f08f2aa ...
[Mar  1 15:10:43]ike_st_i_private: Start
[Mar  1 15:10:43]<none>:500 (Responder) <-> A.A.A.A:500 { f59b44a0 9d324a0b
 0x00000001 } QM; MESSAGE: Phase 2 connection succeeded, No PFS, group = 0
[Mar  1 15:10:43]ike_qm_call_callback: MESSAGE: Phase 2 connection succeeded, No PFS, group = 0
[Mar  1 15:10:43]<none>:500 (Responder) <-> A.A.A.A:500 { f59b44a0 9d324a0b - cab69aaa ef773b06 [0] /
 0x00000001 } QM; MESSAGE: SA[0][0] = ESP aes, life = 102400000 kB/3600 sec, group = 0, tunnel, hmac-
 sha1-96, Extended seq not used,
[Mar  1 15:10:43]ike_qm_call_callback: MESSAGE: SA[0][0] = ESP aes, life = 102400000 kB/3600 sec, group =
 0, tunnel, hmac-sha1-96, Extended seq not used, key len = 256, key rounds = 0
[Mar  1 15:10:43]iked_pm_ipsec_sa_install: local:B.B.B.B, remote:A.A.A.A  IKEv1 for SA-CFG azure_vpn,
 rekey-ikev2:no
[Mar  1 15:10:43]iked_pm_ipsec_sa_create: encr key len 32, auth key len: 20, salt len: 0
[Mar  1 15:10:43]Added (spi=0x224e4032, protocol=ESP dst=B.B.B.B) entry to the peer hash table
[Mar  1 15:10:43]Added (spi=0xb37a4ad0, protocol=ESP dst=A.A.A.A) entry to the peer hash table
[Mar  1 15:10:43]Hardlife timer started for inbound azure_vpn with 3600 seconds/102400000 kilobytes
[Mar  1 15:10:43]Softlife timer started for inbound azure_vpn with 3021 seconds/92160000 kilobytes
[Mar  1 15:10:43]In iked_ipsec_sa_pair_add Adding GENCFG msg with key; Tunnel = 131073;SPI-In = 0x224e4032
[Mar  1 15:10:43]Added dependency on SA config blob with tunnelid = 131073
[Mar  1 15:10:43]Successfully added ipsec SA PAIR
[Mar  1 15:10:43]ike_st_o_qm_wait_done: Marking for waiting for done
[Mar  1 15:10:43]ike_send_notify: Connected, SA = { f59b44a0 9d324a0b - cab69aaa ef773b06}, nego = 0
[Mar  1 15:10:43]IPSec  negotiation done successfully for SA-CFG azure_vpn for local:B.B.B.B,
 remote:A.A.A.A  IKEv1
[Mar  1 15:12:43]ikev2_packet_allocate: Allocated packet 102c000 from freelist
```

Phase2の確立

日本マイクロソフト様の各種リンクと公開情報

Microsoft Azure管理ポータル

- https://manage.windowsazure.com/

仮想ネットワーク概要

- https://msdn.microsoft.com/ja-jp/library/azure/jj156007.aspx

仮想ネットワーク FAQ

- https://msdn.microsoft.com/ja-jp/library/azure/dn133803.aspx

仮想ネットワークに使用する VPN デバイスについて

- https://msdn.microsoft.com/ja-jp/library/azure/jj156075.aspx

everywhere