Orchestrating a brighter world

NEC

UNIVERGE WAシリーズ
Microsoft AzureとのVPN接続 マニュアル

2018年7月31日

NECプラットフォームズ株式会社

Orchestrating a brighter world

未来に向かい、人が生きる、豊かに生きるために欠かせないもの。
それは「安全」「安心」「効率」「公平」という価値が実現された社会です。

NECは、ネットワーク技術とコンピューティング技術をあわせ持つ
類のないインテグレーターとしてリーダーシップを発揮し、
卓越した技術とさまざまな知見やアイデアを融合することで、
世界の国々や地域の人々と協奏しながら、
明るく希望に満ちた暮らしと社会を実現し、未来につなげていきます。

UNIVERGE WAシリーズ Microsoft Azure とのVPN接続

注意事項

- 本資料の設定例は、全て当社で接続を確認しておりますが、
  必ずしも接続性を保証するものではありません。
- 当社は、Microsoft Azureサービスに関連して発生した如何なる障害に対して、
  一切の責任を負わないものとします。
- Microsoft Azureサービスをご利用になる際は、必ず本サービスの利用規約を確認し、
  利用規約に則った運用を行ってください。
- 本資料作成のため、2018年7月上旬にMicrosoft Azureとの動作検証を実施しました。

UNIVERGE WAシリーズ Microsoft Azure とのVPN接続

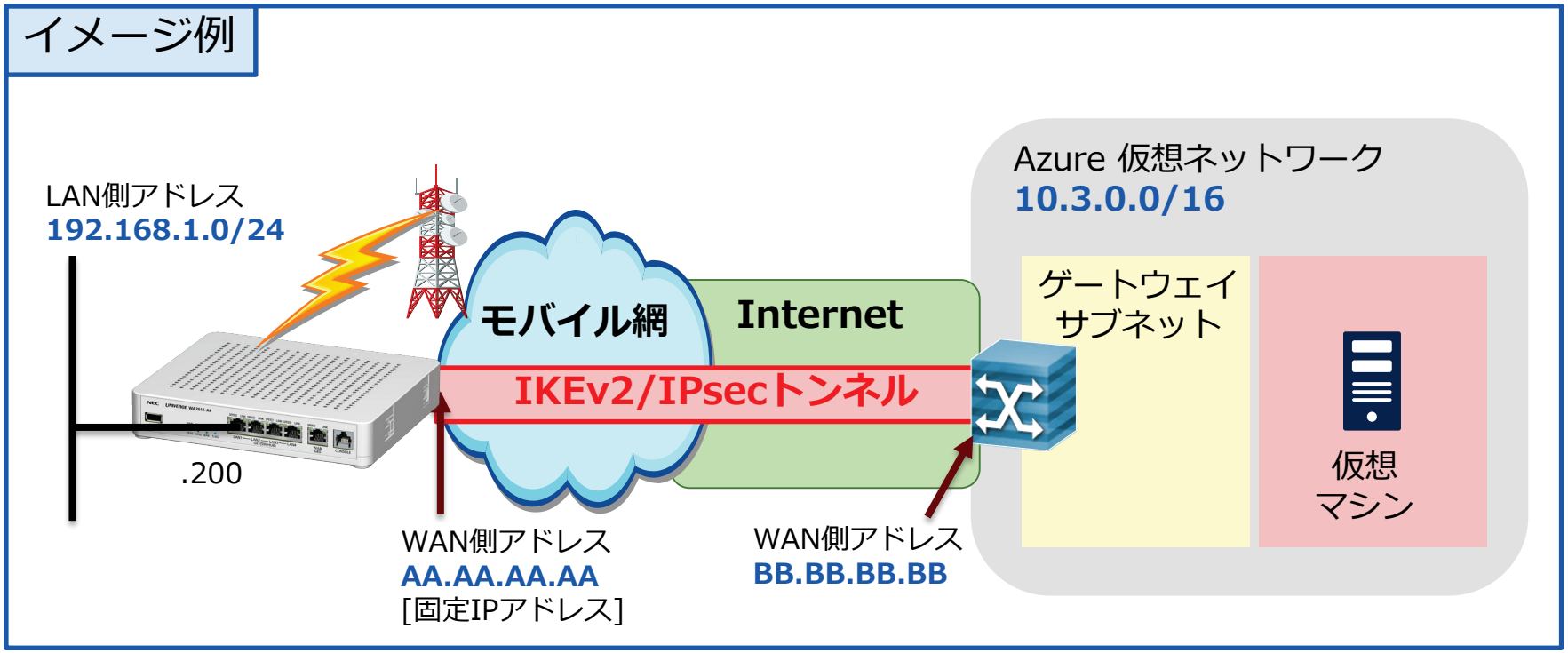
本資料について

「UNIVERGE WAシリーズ」を使用して、
IPsec-VPNで接続する際の設定例を紹介します。
Microsoft Azureでは、サイト間VPNを作成する際、
IPsecゲートウェイの種別として
「ルートベース（動的ルーティング）」 と
「ポリシーベース（静的ルーティング）」
のいずれかを選択する必要があります。
本資料では両方の接続設定例を説明します。
Microsoft Azureサービスをご確認の上、どちらを利用するか判断願います。

ルートベース
（動的ルーティング）

接続構成（ルートベース）

この設定ガイドでは、「WA2612-AP」の**MobileEthernet0.0**をWAN側インタフェース、**GE1(SW-HUB)**ポートをLAN側インタフェースとして使用します。
また、「WA2612-AP」以外の機種（「WA1512など」をご利用の場合でも、本例と同様の設定で接続を行うことができます。



Azure内の仮想ネットワーク及び仮想マシンの設定は、Microsoft Azure Portal サイトで行います。この設定ガイドでは、WA2612-APの設定例についてのみ記載しています。

IPsec設定パラメータ（ルートベース）

以下のパラメータ表に従ってIPsec-VPNの設定を行います。

IPsec	IKEv2
モード	メインモード
IPsecカプセル化モード	トンネルモード
Peerアドレス	**BB.BB.BB.BB** （Microsoft Azureの仮想ネットワークゲートウェイの パブリックIPアドレス）
IKEv2自装置認証の設定	***** （Microsoft Azureに設定した共有キー ※）
IKEv2他装置認証の設定	***** （Microsoft Azureに設定した共有キー ※）
ローカルID	**192.168.1.0**
リモートID	**10.3.0.0**
DHグループ	グループ2 （1,024bit）

※ IKEv2自装置認証とIKEv2他装置認証に設定する共有キーは同じです。

「WA2612-AP」の設定例（ルートベース）

赤字の箇所は、インターネット接続するための設定。Azureとは関係ありません。
青字の箇所は、AzureとVPN接続するための設定です。

1/2

```
interface GigaEthernet1.0
  ip address 192.168.1.200/24
  ip dhcp-server binding default
  no shutdown
!
interface Loopback0.0
  ip address 127.0.0.1/8
  no shutdown
!
interface MobileEthernet0.0
  ip address dhcp
  ip tcp adjust-mss auto
  ip napt enable
  ip napt reserve udp 500
  ip napt reserve esp
  mobile id XX XXXX
  mobile username XXXX
  mobile password plain XXXX
  auto-connect
  no shutdown
!
```

2/2

```
interface IPsec0
  mtu 1350
  ip address unnumbered
  ikev2 binding IKEV2-PROF1
  no shutdown
!
ip route 10.3.0.0/16 IPsec0
ip route default MobileEthernet0.0
!
proxy-dns ip enable
proxy-dns server default MobileEthernet0.0 dhcp
!
!
ikev2 profile IKEV2-PROF1
  ipsec-mode tunnel
  peer BB.BB.BB.BB
  local-authentication psk plain *****
  remote-authentication psk plain *****
  local-id address 192.168.1.0
  remote-id address 10.3.0.0
!
ikev2 default-profile
  source-address MobileEthernet0.0
  dpd interval 10
  sa-proposal dh 1024-bit
!
```

設定完了後の確認（ルートベース）

正常にIPsec SAが確立できていることを確認します。
Inbound/Outbound両方のSAのSPI値、
ライフタイムなどが正しく表示されていることを確認します。

1/2

```
WA2600(config)# show ipsec sa
IPsec SA - 1 configured, 2 created
Interface IPsec0
Outbound:
  AA.AA.AA.AA -> BB.BB.BB.BB
    mode: tunnel
    satype: esp spi=3145487778(0xbb7c55a2)
    enc algorithm: aes-cbc
    key length: 256
    auth algorithm: hmac-sha1-96
    replay window size is 0 bits
    SA status is established
    Remaining lifetime is 28678 seconds
    Remaining lifebytes is - bytes
    0 [packets] 0 [bytes] last:
```

2/2

```
Inbound:
  BB.BB.BB.BB -> AA.AA.AA.AA
    mode: tunnel
    satype: esp spi=174130529(0x0a610561)
    enc algorithm: aes-cbc
    key length: 256
    auth algorithm: hmac-sha1-96
    replay window size is 0 bits
    SA status is established
    Remaining lifetime is 28678 seconds
    Remaining lifebytes is - bytes
    2 [packets] 64 [bytes] last: 3(s) before
```

仮想マシンとの疎通確認

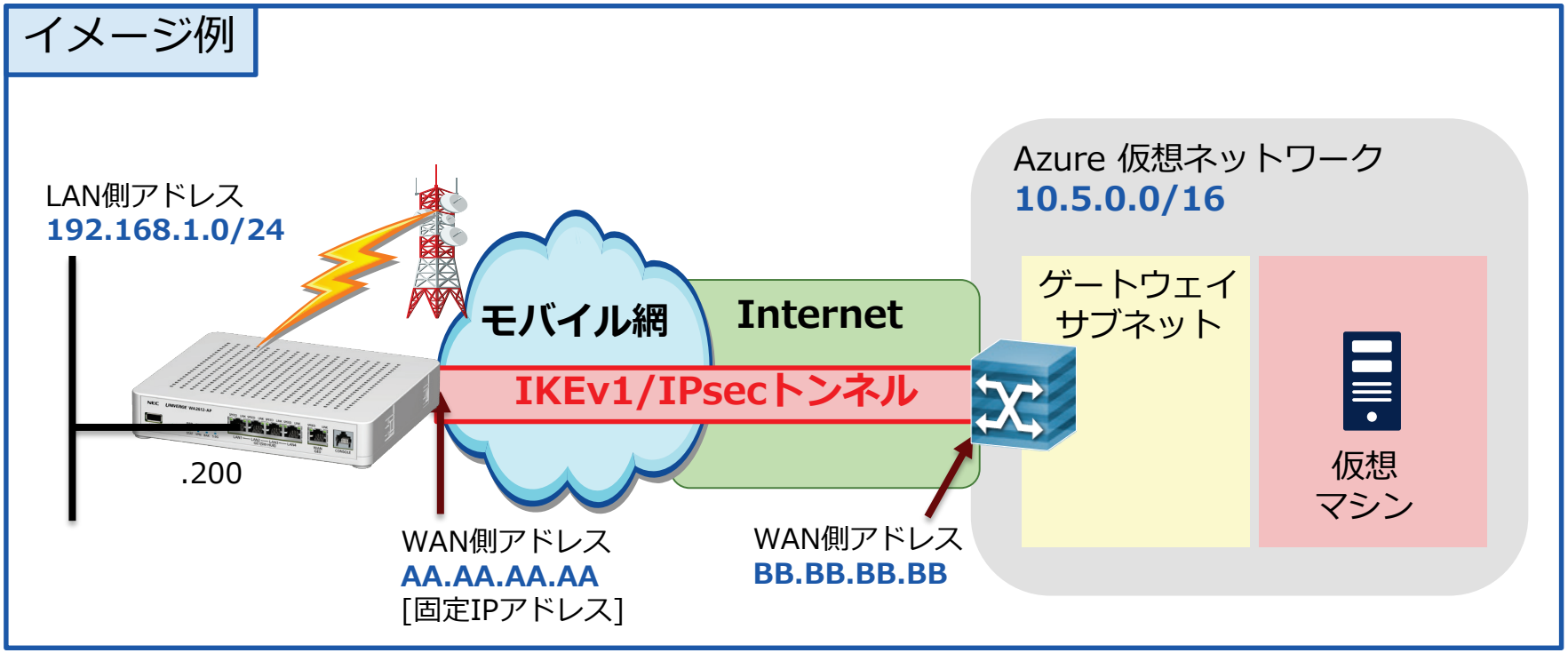
Microsoft Azure上で「仮想マシンに接続する」のRDPを選択し、
WAシリーズ配下のPCから仮想マシンにリモートデスクトップ接続することで、
仮想マシンとの疎通を確認できます。

ポリシーベース（静的ルーティング）

【補足】
Microsoft Azure とのポリシーベースでの接続は、
Web-GUIの「かんたん設定」を利用することで、
WAシリーズに簡単に設定することが可能です。

接続構成（ポリシーベース）

この設定ガイドでは、「WA2612-AP」の**MobileEthernet0.0**をWAN側インタフェース、**GE1(SW-HUB)**ポートをLAN側インタフェースとして使用します。
また、「WA2612-AP」以外の機種（「WA1512など」をご利用の場合でも、本例と同様の設定で接続を行うことができます。



Azure内の仮想ネットワーク及び仮想マシンの設定は、Microsoft Azure Portal サイトで行います。この設定ガイドでは、WA2612-APの設定例についてのみ記載しています。

IPsec設定パラメータ（ポリシーベース）

以下のパラメータ表に従ってIPsec-VPNの設定を行います。

IKE フェーズ1の設定

IPsec	IKEv1
モード	メインモード
事前共有鍵	***** （Microsoft Azureで作成された共有キー）
暗号アルゴリズム	AES256
認証アルゴリズム	SHA2
DHグループ	グループ2 （1,024bit）
ライフタイム	8時間（28,800秒）　※デフォルト

IKE フェーズ2の設定

IPsecカプセル化モード	トンネルモード
暗号アルゴリズム	AES256
Peerアドレス	**BB.BB.BB.BB**（Microsoft Azureの 仮想ネットワークゲートウェイのパブリックIPアドレス）
認証アルゴリズム	SHA2
ライフタイム	1時間（3,600秒）
ローカルID	**192.168.1.0/24**
リモートID	**10.5.0.0/16**

「WA2612-AP」の設定例（ポリシーベース）

赤字の箇所は、インターネット接続するための設定。Azureとは関係ありません。
青字の箇所は、AzureとVPN接続するための設定です。

1/2

```
interface GigaEthernet1.0
  ip address aa.aa.aa.aa/aa
  ip dhcp-server binding default
  no shutdown
!
interface Loopback0.0
  ip address 127.0.0.1/8
  no shutdown
!
interface MobileEthernet0.0
  ip address dhcp
  ip tcp adjust-mss auto
  ip napt enable
  ip napt reserve udp 500
  ip napt reserve esp
  mobile id XX XXXX
  mobile username XXXX
  mobile password plain XXXX
  auto-connect
  no shutdown
!
interface IPsec0
  mtu 1422
  ip address unnumbered
  ip tcp adjust-mss auto
  ipsec map Cloud_IPsec_Profile0
  no shutdown
!
!
ip route 10.5.0.0/16 IPsec0
ip route default MobileEthernet0.0
!
```

2/2

```
!
proxy-dns ip enable
proxy-dns server default MobileEthernet0.0 dhcp
!
!
ike proposal Cloud_IKE_Proposal0
  encryption-algorithm aes256-cbc
  authentication-algorithm hmac-sha2-256
  lifetime 28800
  dh-group 1024-bit
!
ike policy Cloud_IKE_Policy0
  mode main
  dpd-keepalive enable ph1
  proposal Cloud_IKE_Proposal0
  pre-shared-key plain *****
!
!
ipsec proposal Cloud_IPsec_Proposal0
  protocol esp enc-algo aes256-cbc auth-algo hmac-sha2-256
  lifetime 3600
!
ipsec policy Cloud_IPsec_Policy0
  local-id 192.168.1.0/24
  remote-id 10.5.0.0/16
  rekey enable always
  proposal Cloud_IPsec_Proposal0
!
ipsec profile Cloud_IPsec_Profile0
  mode tunnel
  ipsec policy Cloud_IPsec_Policy0
  ike policy Cloud_IKE_Policy0
  peer BB.BB.BB.BB
!
```

設定完了後の確認（ポリシーベース）

正常にIPsec SAが確立できていることを確認します。
Inbound/Outbound両方のSAのSPI値、
ライフタイムなどが正しく表示されていることを確認します。

1/2

```
WA2600(config)# show ipsec sa
IPsec SA - 1 configured, 2 created
Interface IPsec0
Outbound:
  AA.AA.AA.AA -> BB.BB.BB.BB
    mode: tunnel
    satype: esp spi=4154409688(0xf79f42d8)
    enc algorithm: aes-cbc
    key length: 256
    auth algorithm: hmac-sha2-256
    replay window size is 0 bits
    SA status is established
    Remaining lifetime is 3503 seconds
    Remaining lifebytes is - bytes
    0 [packets] 0 [bytes] last:
```

2/2

```
Inbound:
  BB.BB.BB.BB -> AA.AA.AA.AA
    mode: tunnel
    satype: esp spi=152504919(0x09170a57)
    enc algorithm: aes-cbc
    key length: 256
    auth algorithm: hmac-sha2-256
    replay window size is 0 bits
    SA status is established
    Remaining lifetime is 3503 seconds
    Remaining lifebytes is - bytes
    2 [packets] 64 [bytes] last: 19(s) before
```

仮想マシンとの疎通確認

Microsoft Azure上で「仮想マシンに接続する」のRDPを選択し、
WAシリーズ配下のPCから仮想マシンにリモートデスクトップ接続することで、
仮想マシンとの疎通を確認できます。

UNIVERGE WAシリーズ
Microsoft AzureとのVPN接続 マニュアル

GVT-075232-001-00

2018年7月　第7.5版
NECプラットフォームズ株式会社
（禁無断複製）


Orchestrating a brighter world
NEC