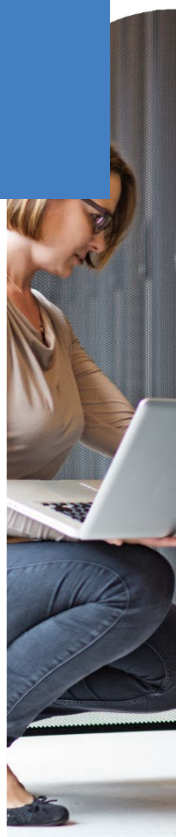
DEPLOYMENT GUIDE

FortiGate IPoE設定ガイド

アルテリア・ネットワークス株式会社

クロスパス 可変IPサービス編

Version 1.0.0 2022年5月



免責事項

また本内容は参考例となります。個別のセキュリティ対策に関する要件を満たすには、ご利用者様ごとにプランニングおよび設定の調整が必要となりますので、予めご了承下さい。尚、本ドキュメントの作成にあたっては細心の注意を払っておりますが、その記述内容は予告なしに変更される事があります。

目次

第1章：はじめに 4

第2章：FortiGateの設定 7

第3章：動作確認方法 14

改定履歴 16

1. はじめに

この設定ガイドはアルテリア・ネットワークス株式会社が提供するクロスパス IPv4インターネット接続 IPoE（IPv4可変）でFortiGateを宅内ルータとして利用する際の基本的な設定について説明しています。

クロスパスや対応端末に関してはアルテリア・ネットワークス株式会社のホームページをご参照ください。
https://www.arteria-net.com/business/service/internet/line/flets/
https://www.arteria-net.com/files/user/images/business/service/internet/xpass_ipv6.pdf

対応しているサービスは可変IP方式、固定IP方式のサービスになります。ご利用のサービスに該当する設定ガイドを参照し設定を行ってください。

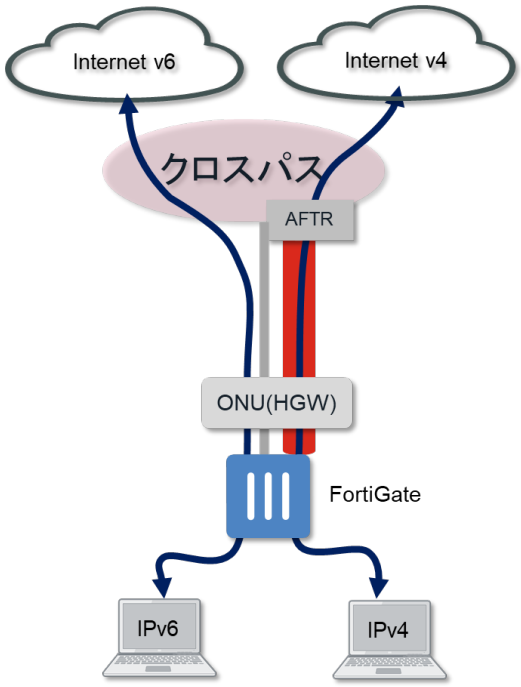
本ガイドでご紹介している機能はFOS7.2.0以上のバージョンが必要になります。以前のバージョンをご利用の場合は予めFortiGateのバージョンアップを実施してください。ファームウェアのアップグレードパスやアップグレード方法に関してはリリースノートやマニュアルなどをご参照ください。

本ガイドの設定はFortiGate 60Fで記載しています。インターフェース名など機器に依存する箇所に関してはお使いのFortiGateに合わせて設定してください。

本ガイド執筆時のバージョンではご紹介の機能はCLIからのみの設定となります。ポリシー設定など一部既存機能等はGUIでも設定可能ですが本ガイドでは設定はCLIで記載しております。

本ガイドでのIPv4アドレスは疑似環境で行っているためプライベートIPアドレスを使用しております。

接続イメージ



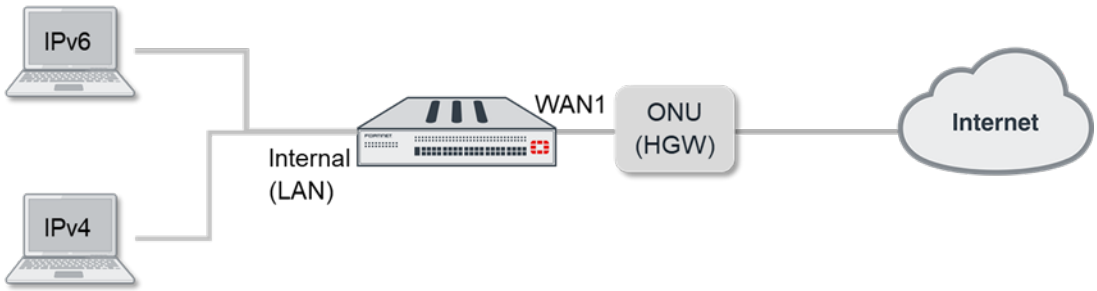
1-1. 利用機器と OS バージョン

FortiGate　FortiGate 60F　7.2.0

1-2. 構成

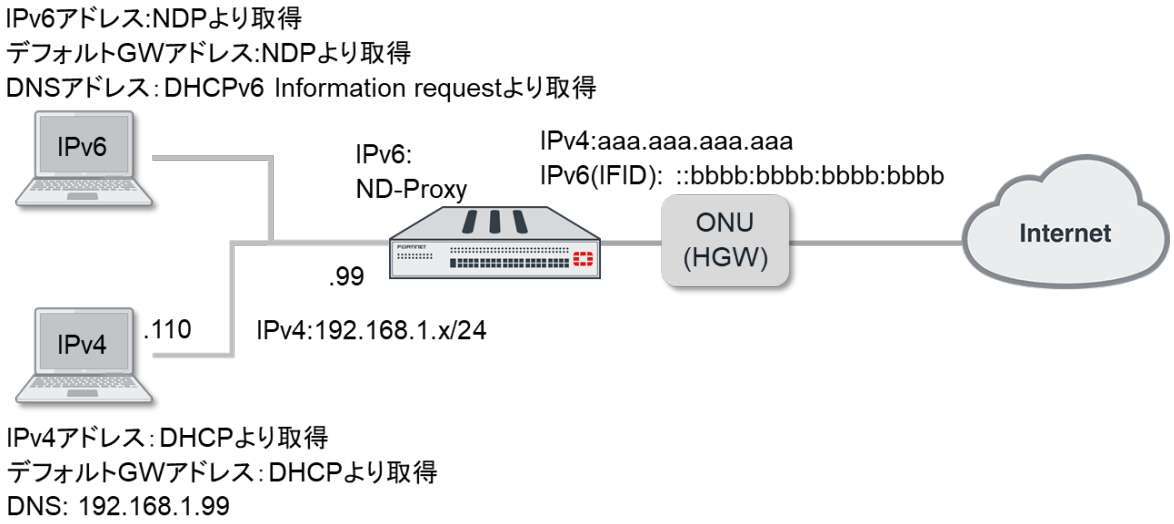
HGWの配下にFortiGateを設置する際はHGWのLANポートに接続してください。HGWのLANポートでDHCPが有効になっている場合は無効に設定して頂くかHGWに接続するFortiGateポート（本ガイドではWAN1）ではDHCPでのアドレス取得を無効にして下さい。

物理構成



<図1-2-1. 物理構成図>

論理構成



<図1-2-2. 論理構成図>

1-3. 参考資料

本設定ガイドは公式な設定ガイドに基づいています。より詳細な情報が必要な場合は以下も合わせてご参照ください。

https://docs.fortinet.com/document/fortigate/7.2.0/administration-guide/954635/getting-started

FortiGateとパソコンなど設定用端末の接続に関してはシリアルコンソールなどで接続してください。接続方法など詳細な情報が必要な場合は以下も合わせてご参照ください。

https://docs.fortinet.com/document/fortigate/7.2.0/administration-guide/901037/connecting-to-the-cli

2. FortiGate の設定

2-1. WAN1 インターフェースの IPv6 の設定

CLIより WAN1インターフェースに以下の項目を設定します。

HGWの配下にFortiGateを設置する場合でかつHGWでDHCPv4サーバが有効な場合は以下のとおりset mode staticも設定して下さい。

```
config system interface
    edit wan1
        set mode static
        config ipv6
            set dhcp6-information-request enable
            set autoconf enable
            set unique-autoconf-addr enable
        end
    next
end
```

2-2. トンネルインターフェースの有効化

CLIより vne-tunnelの項目で以下の設定を行います。modeにはds-liteを設定してください。brには可変サービスご契約時に案内されるAFTRのFQDNを指定して下さい。可変方式ではIPv4のアドレスの指定はございませんが、FortiGateが自発パケットをvne.rootインターフェースで送信する場合にIPv4アドレスの設定が必要となります。ご利用になっていないプライベートIPアドレスを設定することをおすすめいたします。FortiGateは設定されたプライベートIPv4アドレスでIPv4インターネットにアクセスいたしますが、クロスパス網にてNATが行われるためIPv4でのインターネットアクセスが可能です。

```
config system vne-tunnel
    set status enable
    set interface "wan1"
    set mode ds-lite
    set ipv4-address 192.168.255.255 255.255.255.255
    set br "XXX.XXXX.XX"
end
```

2-3. デフォルト DNS 設定の削除（オプション）

「DNSサーバとしてDHCPv6 information requestで取得したサーバを利用する為デフォルトの設定を削除します。

```
config system dns
    unset primary
    unset secondary
end
```

2-4. DNS サーバの設定（オプション）

internal インターフェースにDNSサーバ recursiveモードの設定を行います。設定したinternalインターフェースでDNSサーバの機能が有効になります。

```
config system dns-server
    edit internal
    next
end
```

2-5. IPv4 ポリシーの作成

CLIによりinternalインターフェースからトンネルインターフェース（vne.root）宛のIPv4ファイアウォールポリシー設定を行います。dstintfはトンネルインターフェースのvne.rootを選択します。アドレスやサービス等は実際の構成に合わせてください。本ガイドでは説明を簡単にするために全てを許可と設定しています。

```
config firewall policy
    edit 1
        set name internal-to-vne.root
        set srcintf internal
        set dstintf vne.root
        set srcaddr all
        set dstaddr all
        set action accept
        set schedule always
        set service ALL
        set tcp-mss-sender 1420
        set tcp-mss-receiver 1420
        set nat enable
    next
end
```

2-6. デフォルトルートの設定

トンネルインターフェースのvne.rootをデフォルトルートとして設定します。

```
config route static
    edit 1
        set device vne.root
    next
end
```

2-7. IPv6 Neighbor Discover Proxy 機能の有効化（オプション）

下記のコマンドでIPv6 Neighbor Discover Proxyの機能をwan1、internal間で有効にします。

FortiGate配下のクライアントからIPv6インターネットに接続する必要がない場合、以降の設定は必要ございません。

```
config system nd-proxy
    set status enable
    set member wan1 internal
end
```

2-8. IPv6 ポリシーの作成 （オプション）

ICMPv6,DHCPv6を許可させる為にv6マルチキャストポリシーと、IPv6アドレスオブジェクト、v6ポリシーを作成します。下記にてinternalインターフェースとwan1インターフェース双方向のマルチキャスト通信を許可するIPv6マルチキャストファイアウォールポリシーを設定します。

```
config firewall multicast-policy6
    edit 1
        set srcintf wan1
        set dstintf internal
        set srcaddr all
        set dstaddr all
    next
    edit 2
        set srcintf internal
        set dstintf wan1
        set srcaddr all
        set dstaddr all
    next
end
```

次に、IPv6ユニキャストファイアウォールポリシーを作成します。
まず、リンクローカルIPv6アドレスオブジェクトを作成します。

```
config firewall address6
    edit link-local
        set ip6 fe80::/64
    next
end
```

internalインターフェースからwan1インターフェース宛の通信を許可するファイアウォールポリシー、wan1インターフェースからinternalインターフェースへのリンクローカルアドレスでの通信を許可するファイアウォールポリシーを作成します。wan1インターフェースからinternalインターフェースへのその他の通信（インターネットからのアクセス）も許可したい場合は環境に合わせて設定ください。

```
config firewall policy
      edit 11
        set name internal-to-wan1
        set srcintf internal
        set dstintf wan1
        set srcaddr6 all
        set dstaddr6 all
        set action accept
        set schedule always
        set service ALL
    next
    edit 12
        set name wan1-to-internal
         set srcintf wan1
        set dstintf internal
        set srcaddr6 link-local
        set dstaddr6 link-local
        set action accept
        set schedule always
        set service ALL
    next
end
```

3. 動作確認方法

3-1. IPv6 トンネルの確認

AFTRとIPv6トンネルが確立できていることを確認します。

```
# diagnose ipv6 ipv6-tunnel list
```

laddrにFortiGateのIPv6アドレス、raddrにAFTRのIPv6アドレスが記載され、rxやtxのバイト数やパケット数がカウントされていることを確認します。

```
# diagnose ipv6 ipv6-tunnel list
devname=vne.root devindex=5 ifindex=24 vfid=0000 ref= 0
laddr= XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX raddr=XXXX:XXXX:XXXX::X
  RX bytes:2865221 (2.7 Mb)   TX bytes:348609 (340.4 kb);
  RX packets:2294, TX packets:2935, TX carrier_err:0 collisions:0
  npu-info: asic_offload=1, enc4/dec4=1/0,  enc6/dec6=0/0,
  enc4_bk=-1/6/64, dec4_bk=0/0/0, enc6_bk=0/0/0, dec6_bk=0/0/0
  rpdb-ver: ffffffff rpdb-gwy: :: rpdb-oif: 0
total tunnel = 1
```

3-2. IPv4 でのインターネットアクセス確認

IPv4でのインターネットアクセスが可能かIPv4 pingなどで確認します。

```
# execute ping example.com
PING example.com (X.X.X.X): 56 data bytes
64 bytes from X.X.X.X: icmp_seq=0 ttl=53 time=3.3 ms
64 bytes from X.X.X.X: icmp_seq=1 ttl=53 time=2.7 ms
64 bytes from X.X.X.X: icmp_seq=2 ttl=53 time=3.1 ms
64 bytes from X.X.X.X: icmp_seq=3 ttl=53 time=3.3 ms
64 bytes from X.X.X.X: icmp_seq=4 ttl=53 time=2.7 ms
```

改定履歴

バージョン	リリース日	改定履歴
1.0.0	2022.5	初版発行