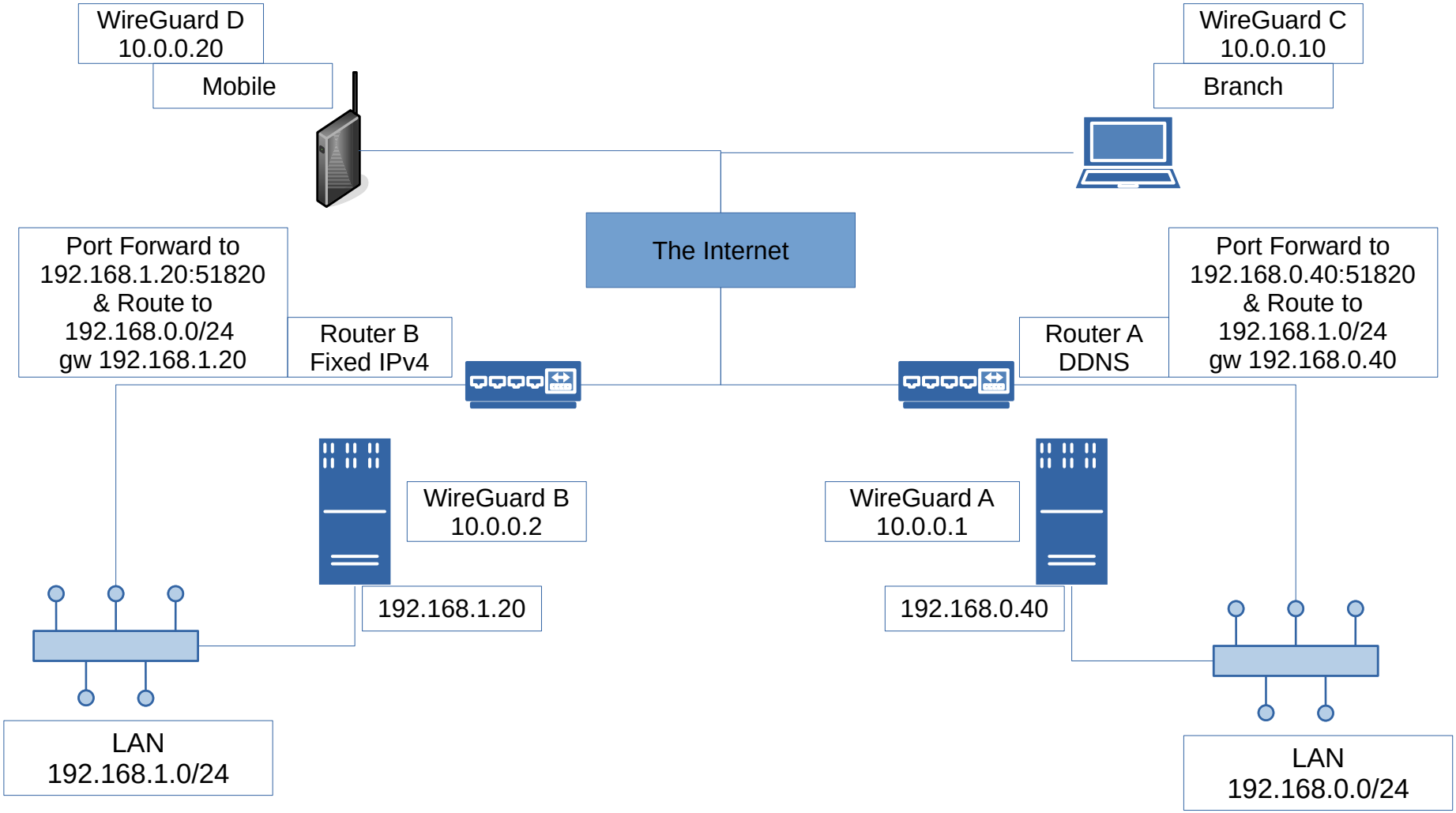
WireGuard VPN テスト



2022/4/22 setter at i-red dot info

WireGuard A, B 共通でやること

Wireguard のインストール（Ubuntu20.04）

```
# apt install wireguard
```

Linux Kernel の設定（フォワーディング）

*/etc/*sysctl.conf に以下の行を追加
net.ipv4.ip_forward=1
# sysctl -p

WireGuard の鍵の作成（）

```
# cd /etc/wireguard
# wg genkey > sv_prvkey
# wg pubkey < ./sv_prvkey > ./sv_pubkey
# wg genkey > cl_prvkey
# wg pubkey < ./cl_prvkey > ./cl_pubkey
# chmod 600 ./*key
```

インタフェース名の確認（WireGuard の設定で使う）
eth0 とか enp2云々とか言う名前のはず

```
$ ip a
```

RouterA の設定

WireGuard A（192.168.0.40）にポート番号 51820 をフォワード（静的IPマスカレード）する。

192.168.1.0/255.255.255.0 宛のゲートウェイを 192.168.0.40 （静的ルーティング）にする。

RouterB の設定

WireGuard B（192.168.1.20）にポート番号 51820 をフォワード（静的IPマスカレード）する。

192.168.0.0/255.255.255.0 宛のゲートウェイを 192.168.1.20 （静的ルーティング）にする。

（WireGuard A の設定）

vi /etc/wireguard/wg0.conf

[Interface]
PrivateKey = （/etc/wireguard/sv_prvkeyの中身を書く）
Address = 10.0.0.1　（WireGuard の IF アドレス）
ListenPort = 51820（192.168.0.40 での listen ポート）
MTU = 1392

（wg0 有効時 に インタフェース（enp0s3）への nat を設定）
PostUp = iptables -A FORWARD -i wg0 -j ACCEPT
PostUp = iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE

（wg0 無効化時 に インタフェース（enp0s3）への nat を解除）
PostDown = iptables -D FORWARD -i wg0 -j ACCEPT
PostDown = iptables -t nat -D POSTROUTING -o enp0s3 -j MASQUERADE

[Peer]（WireGuard Bとの拠点間通信）
PublicKey = （WireGuard B の/etc/wireguard/sv_pubkeyの中身を書く）
AllowedIPs = 10.0.0.0/24, 192.168.1.0/24（通信を許可するアドレス）
Endpoint = RouterBのグローバルIPアドレス:51820
PersistentKeepalive = 25

[Peer]（Home PC）
PublicKey = （WireGuard A の/etc/wireguard/cl_pubkeyの中身を書く）
AllowedIPs = 10.0.0.10/32

（コメントは削除しないと多分動かないよ）

設定を保存したら、パーミッション変えとく。
chmod 600 /etc/wireguard/wg0.conf

WireGuard を起動する
wg-quick up wg0
wg

（WireGuard B の設定）

vi /etc/wireguard/wg0.conf

[Interface]
PrivateKey = （/etc/wireguard/sv_prvkeyの中身を書く）
Address = 10.0.0.2
ListenPort = 51820
MTU = 1392

PostUp = iptables -A FORWARD -i wg0 -j ACCEPT
PostUp = iptables -t nat -A POSTROUTING -o enp2s0 -j MASQUERADE

PostDown = iptables -D FORWARD -i wg0 -j ACCEPT
PostDown = iptables -t nat -D POSTROUTING -o enp2s0 -j MASQUERADE

[Peer]（WireGuard A との拠点間通信）
PublicKey = （WireGuard A の/etc/wireguard/sv_pubkeyの中身を書く）
AllowedIPs = 10.0.0.0/24, 192.168.0.0/24
Endpoint = RouterAのドメイン名:51820
PersistentKeepalive = 25

[Peer]（Mobile）
PublicKey = （WireGuard B の/etc/wireguard/cl_pubkeyの中身を書く）
AllowedIPs = 10.0.0.20/32

（コメントは削除しないと多分動かないよ）

chmod 600 /etc/wireguard/wg0.conf

wg-quick up wg0
wg

MTU は VPN 開通したら、ping -M do -s 1420 あたりから減らしていってエラーが無くなるとこ探す。適正値にしないとすごく遅くなるかも。

（WireGuard C（Windows10）での設定）

[Interface]
PrivateKey = （WireGuard A の /etc/wireguard/cl_prvkeyの中身を書く）
Address = 10.0.0.10
MTU = 1392

[Peer]（WireGuard A 用）
PublicKey = （WireGuard A の/etc/wireguard/sv_pubkeyの中身を書く）
AllowedIPs = 10.0.0.0/24, 192.168.0.0/24, 192.168.1.0/24
Endpoint = RouterAのドメイン名:51820

（WireGuard D（モバイルやったことない）での設定）

[Interface]
PrivateKey = （WireGuard B の /etc/wireguard/cl_prvkeyの中身を書く）
Address = 10.0.0.20
MTU = 1392

[Peer]（WireGuard B 用）
PublicKey = （WireGuard B の/etc/wireguard/sv_pubkeyの中身を書く）
AllowedIPs = 10.0.0.0/24, 192.168.1.0/24, 192.168.0.0/24
Endpoint = RouterBのグローバルIPアドレス:51820