2024/4/13VPNハンズオン

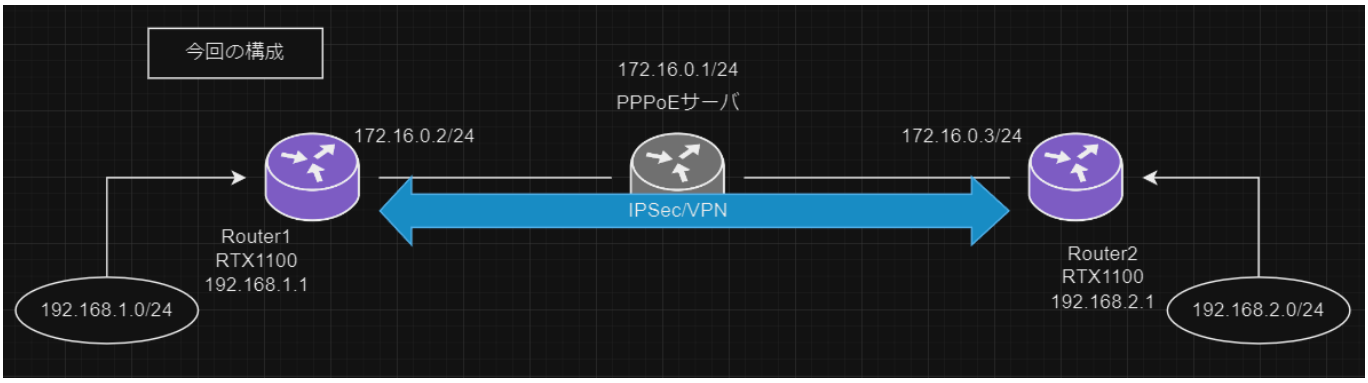
アジェンダ

- IPSEC/VPNのお時間
  - 通常のIPSec/VPN（ESP暗号化）での通信
  - 認証のみのAHでの通信
  - パケットキャプチャをする

登場人物

- RTX1100
- Cisco 3825（PPPoEサーバー）

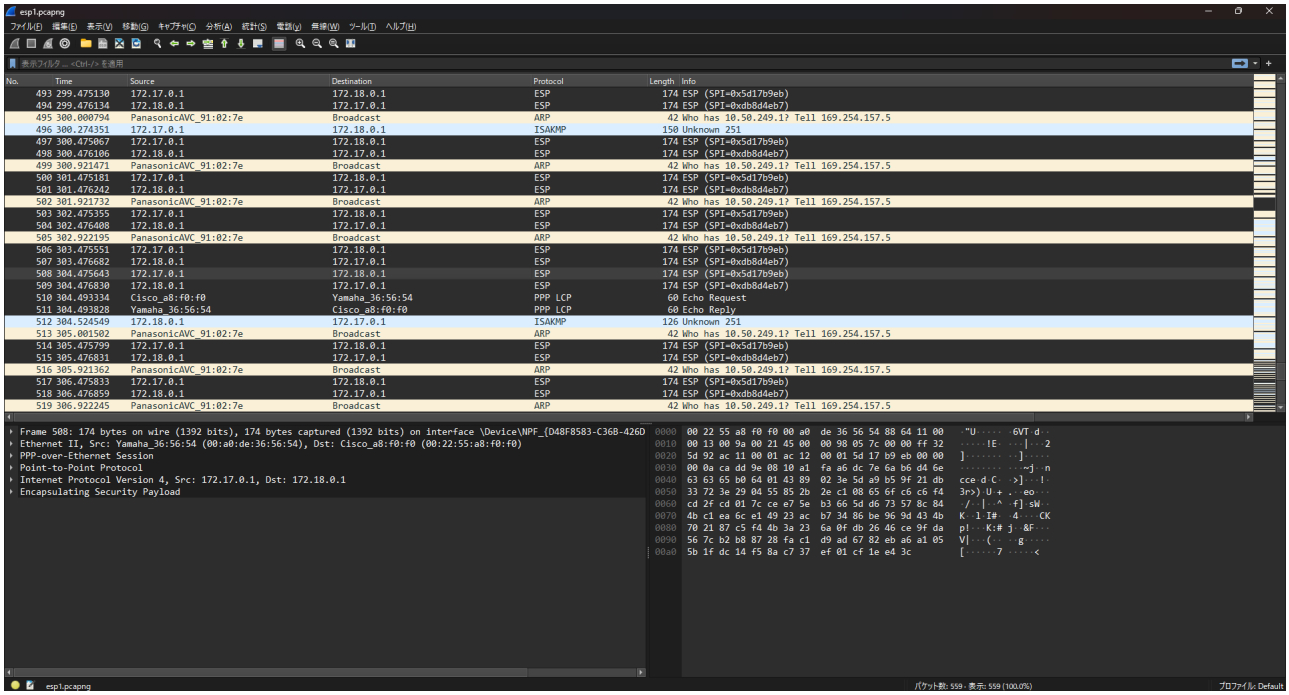
簡単な構成図



国内でよくあると思う構成を考えました。
RTX1100同士をPPPoE接続を行った上でIPSec/VPNをする。
PPPoEインターフェースではNAPTをする。
Wiresharkでパケットキャプチャをする。RTX1100とPPPoEサーバーの間にリピータハブでノートパソコンを接続しキャプチャした。
ちなみに、PCをPPPoEサーバーに接続し、PPPoEでダイヤルアップをすると接続できる。

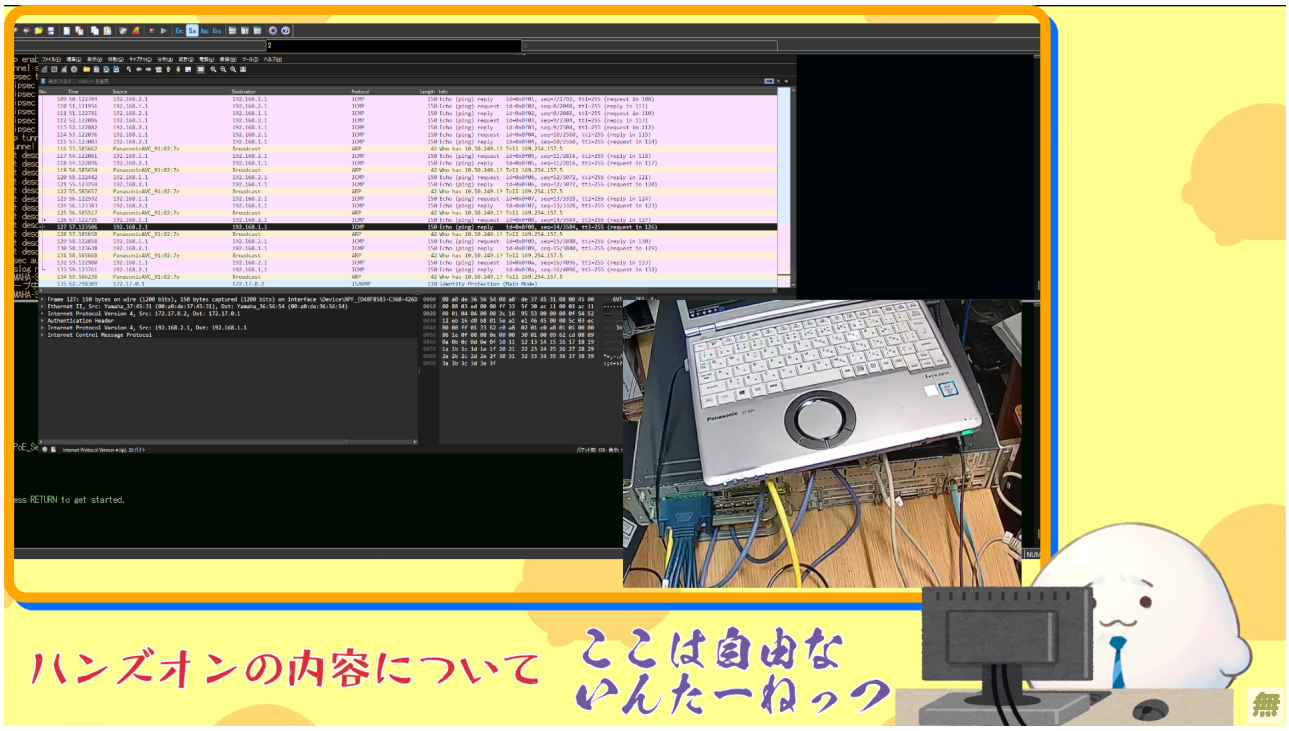
所感

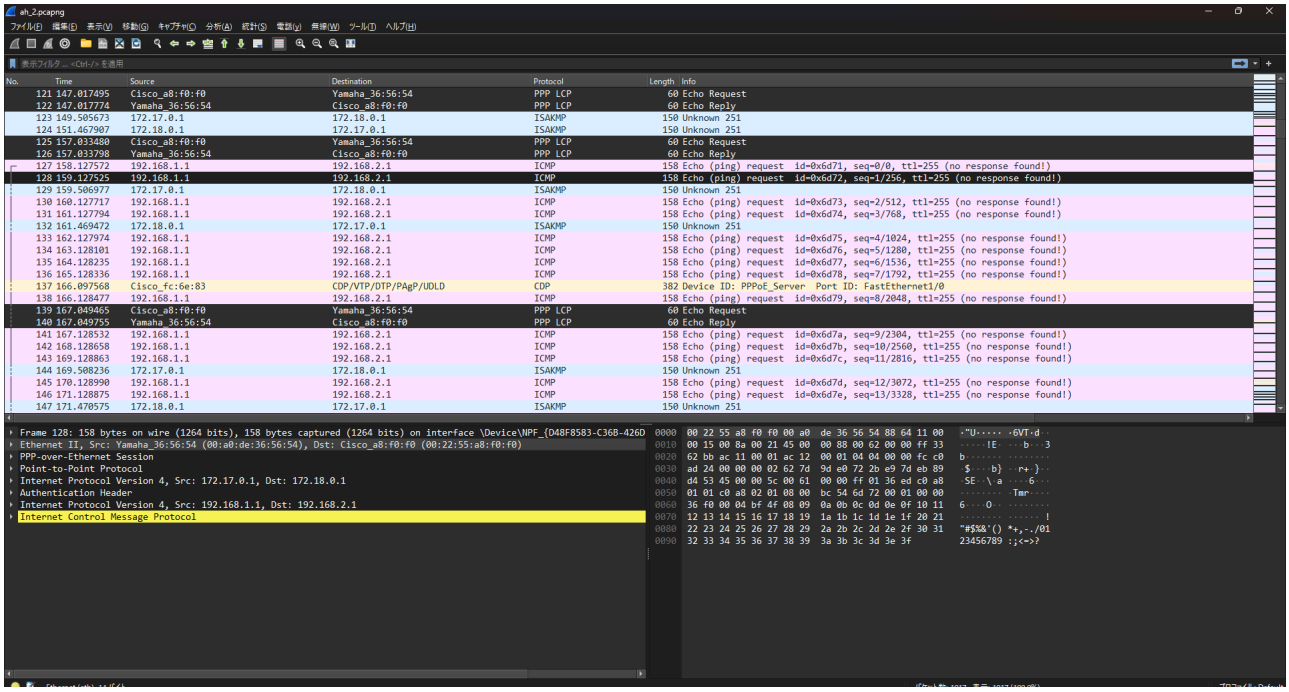
- ESPでの暗号化を使用したIPSec/VPNはすんなりつながった。



暗号化されているパケットの様子

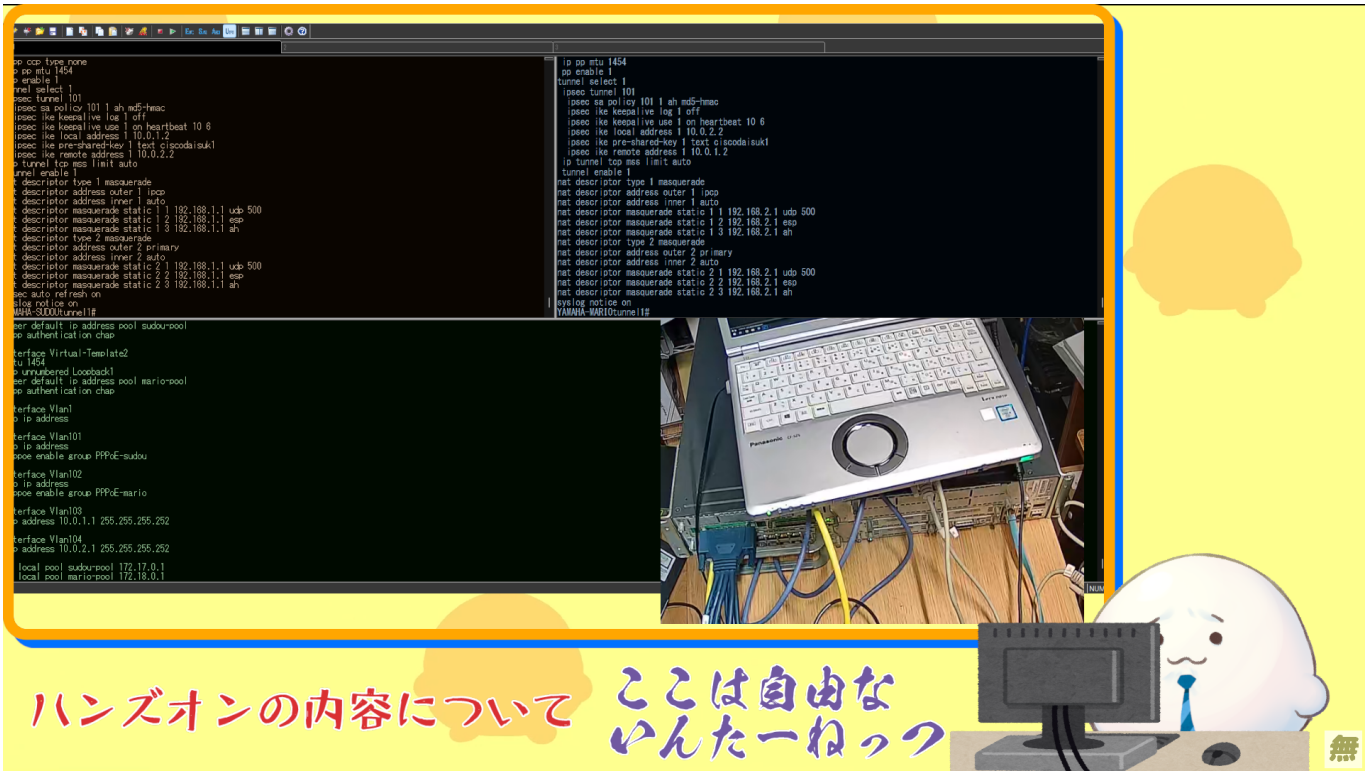
- AHのみのVPNはトンネルがつながるものの通信はできなかった。
- パケットキャプチャをするとESPの場合は暗号化がされており読めない状態だが、AHの場合はどういうわけかAHヘッダの後にあるIPアドレスを使用して通信を行ってしまう模様（理由不明）





- AHのみの採用例も見当たらず、設定例もないため断念。
  - 考察
    - NAPTをしている関係上、DestIPアドレスがAHヘッダの後にあるIPアドレス（LAN内IPアドレス）になっているとNAPTで弾かれてしまう？
    - NAPTをしている関係上、IPアドレスが変わっているように見えるため改ざんされているとして相手をしない？（理由として濃厚）
    - LAN同士をつなぎ、NAPTをはずすと通信可能
      - →NAPTをするルーターをAHするルーターの前に置くと通信可能…？
  - そもそも「IPヘッダ|AHヘッダ|LAN内IPヘッダ|TCP/UDPヘッダ…」と頭にIPヘッダがあるのになぜわざわざAHヘッダの後のIPヘッダが読まれるのか不明。（IPヘッダも含めて認証に使われる関係？）
  - これがYAMAHAのルーターの挙動のせいかのかどうなのかが判断がつかないので、後日別のメーカーのルーターでも試してみる。
  - とにかく情報がないのであまり手も足も出ない。

雑感



- VPN接続を行った際のフレームフォーマットについてよく考えることができた。
- IKE、ESP、AHの関係がわかった。
- 知識的にあることは知っていたAHについて触れることが出来た。
- パケットキャプチャをすることにより、TELNET使用時のパケットの動き、Pingをした際のパケットの動きを確認しながらVPNの効果を確認できた。
- とっつきにくい印象のVPNを触ることにより多少は仲良くなれた気がする。