OpenVPN を用いた個別 VLAN 接続サービスの構築

針木 剛 [1)]

1) 京都大学 企画・情報部

hariki.tsuyoshi.3r@kyoto-u.ac.jp

construction of connecting to indivisial VLAN service by using OpenVPN

HARIKI Tsuyoshi[1)]

1) Information Dept., Kyoto Univ.

概要

京都大学では複数の VPN サービスを運用しておりその 1 つとして OpenVPN サービスを提供している。Windows や macOS の OS 標準機能である IKEv2 サービスを主たる VPN サービスとしているが、利用者のネットワーク環境のフィルタ等が原因で接続不可といった場合の受け皿として TCP の 443 番ポートで運用する OpenVPN を利用して頂いている。本稿では IKEv2 で既に提供している研究室など個別 VLAN への接続機能を OpenVPN にも同様に実装した際の各種設定方法や得られた知見の情報共有を目的として詳細内容をまとめる。

1 はじめに

京都大学では IKEv2 サービスを主たる VPN サービスとして運用している [1] が、IPsec のために UDP の 500 番ポートと ESP または NAT 配下の端末であれば UDP の 4500 番ポートが利用できるネットワーク環境が必要となる。従来よりネットワークの通信フィルタ等が原因で利用不可となるケースがあったが、特に IPv6 のみといったネットワーク環境の増加に伴い IPv4 で運用している IKEv2 サーバとの通信ができないといった利用者からの問い合わせも増えていることから対応を検討した。

また京都大学では歴史的経緯から 4 つの VPN サービスを運用しているが、システム更新を控えコスト削減が求められる中でこれらを一旦整理して運用コスト面からも総合的にどのような解決方法があるか検討を行った。

2 学内ネットワーク環境

京都大学では学内関係者が研究室 VLAN でパソコンやプリンタを利用するためのプライベートアドレス「KUINS-III」と、学外への通信や学外公開のためのグローバルアドレス「KUINS-II」を運用している。教職員は希望に応じて「KUINS-DB」と呼ばれる Web フォームからそれらを利用申請し、申請内容を保存したデータベースの内容を適宜ネットワーク機器の設定に反映することで運用を行っている。また大学を地理的に 10 構内に分割し各構内に L3 スイッチを配置し大学全体を束ねる主たる L3 スイッチでそれぞれのルーティングを管理する構成となっている。各構内で利用する VLAN 数が多いため各構内の L3 スイッチごとに独立した VLAN 番号を割り当てている。そのため VLAN 番号とは別に学内で一意の値となる「VLAN 管理番号」を別途割り当て「KUINS-DB」で管理している。「KUINS-DB」の各 VLAN には「全学アカウント」と呼ばれる大学構成員全員に割り当てられた認証 ID が登録可能である。VPN や無線 LAN 利用時の認証 ID を「全学アカウント@VLAN 管理番号」とすることでその VLAN に接続できるようになっている [2]。

3 VPN サービス比較検討

現在京都大学では学外からの安全な通信経路の提供を目的として 4 つの VPN サービスを提供している。VPN サービスを提供し始めた 2005 年度当時 Windows 端末で安定動作が可能であった PPTP サービスを選択し、学内限定の事務手続きサイトや接続元が大学の IP アドレスに限定される電子ジャーナルの閲覧など多くの教職員や学生など学内関係者に利用されてきた。

一方で PPTP 接続時の GRE プロトコルが利用者環

境によって制限されている場合もあり、その代替策として 2012 年度に TCP のみで利用できる SSTP サービス及び OpenVPN サービスを開始した。

また Apple 社が 2016 年 9 月に提供する新しい iOS や macOS で PPTP を非サポートとする通知があり、これに対応するため新たに IKEv2 サービスの運用を開始した。

表 1 に利用者のネットワーク環境で必要となるプロトコルやポート番号、また表 2 に各 VPN の端末 OS での対応一覧をまとめる。

表 1　VPN に必要なプロトコルやポート番号比較

IKEv2	○ (500/UDP と (ESP または 4500/UDP))
PPTP	△ (1703/TCP と GRE)
SSTP	◎ (443/TCP)
OpenVPN	○ (1194/UDP)*1

*1 京都大学では 443/TCP で運用

表 2　VPN クライアント OS 対応比較

	Windows	macOS	iOS	Android
IKEv2	○	○	○	△
PPTP	○	×	×	× *1
SSTP	○	×	×	×
OpenVPN	△	△	△	△

○...OS 標準対応　△... アプリ対応　× ... 非対応

*1 クライアント証明書認証不可のため

利用者の手間を最小限にするために極力クライアント OS 標準対応しているものが望ましく、利用者には IKEv2 の利用を推奨している。ただしネットワーク環境により利用不可である場合は SSTP や OpenVPN を利用するようお願いしている。

また京都大学の運用ポリシーとして有効にしている認証方式と、研究室や事務室などの閉じた VLAN(以下個別 VLAN とする) へ直接接続できる機能の有無を表 3 にまとめる。

表 3　認証方式と個別 VLAN 接続機能

	パスワード認証	証明書認証	個別 VLAN
IKEv2	○	○	○
PPTP	×	○	○
SSTP	×	○	×
OpenVPN	×	○	×

PPTP サービス及びその代替である IKEv2 サービスは開始当初は全ての機能を有効としたが、PPTP はパスワード認証の脆弱性から証明書認証限定に変更している。補助的なサービスである SSTP と OpenVPN は開始当初から機能を制限して運用している。

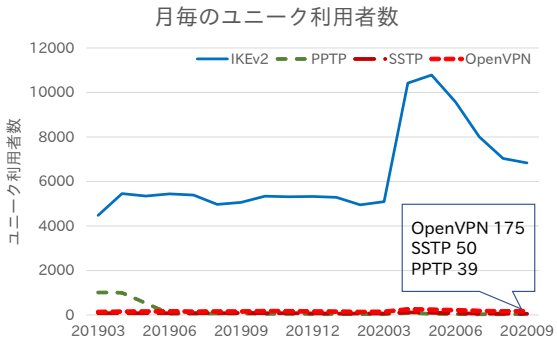

図 1　VPN サービスユニーク利用者数の推移

図 1 に直近の利用者数の推移を示す。

PPTP はパスワード認証制限時に利用者数は減少し、IKEv2 の利用が増加している。また 2020 年度は全学的に教職員の在宅勤務が推奨され全ての VPN サービスの利用者数が増えているがその中で IKEv2 の利用が大幅に伸びていることが分かる。

加えて利用できる OS が限定される PPTP や SSTP については各種 OS で利用可能な OpenVPN に比べ利用者数が少ないことが分かる。

これらの利用状況を鑑み、今後の運用コスト抑制のため次期システム更新時にはこの PPTP 及び SSTP の VPN サービスを廃止し、主たるサービスとしての IKEv2 と補助的なサービスとしての OpenVPN の 2 つを今後の VPN サービスとする方針とした。

両サービスの利用者には Web サイトの通知以外にも個別にメール連絡する予定であるが、同時に従来のサービスレベルの維持に配慮しなければならない。

特に個別 VLAN への接続機能を実装しているサービスが IKEv2 と PPTP のみであり、ネットワーク環境として PPTP は利用可であるが IKEv2 が利用不可といった利用者も少なからず存在するため、その対応を検討する必要がある。

例えば受け皿サービスとしての OpenVPN の機能強化として個別 VLAN の接続機能を実装することで、それらの利用者も従来どおり研究室等に接続することが可能と思われる。

また 1 節にあるとおり IKEv2 が利用できないネットワーク環境も増えており、研究室の情報リソースに接続したいが自宅環境では接続できないといった要望も増えていることから、今後 2 本柱で VPN サービスを運用する上でも OpenVPN の個別 VLAN 接続機能には高い需要があると考えている。

一方でパスワード認証機能についてはパスワードのみの認証で十分な安全性を確保することが難しいことから、将来的に IKEv2 側のパスワード認証機能を停止することも検討している。

4　システム構築

4.1　システムの動作詳細

サーバは新規構築して、従来の個別 VLAN に接続しない共通 VLAN 方式のサーバと個別 VLAN 方式のサーバの両者を稼働させる。

共通 VLAN 方式は下記の接続フローとなる。

1. 利用者の端末から OpenVPN サーバの KUINS-II へのアクセスに対し、NII のクライアント証明書認証を行い、Subject から京都大学で発行申請された証明書と判定されると端末に KUINS-III ではないプライベート IP アドレスを割り当てる。
2. 京都大学 IP アドレスの接続元制限で運用される学外サイトのため、すべての通信が VPN を経由するようにルーティングをプッシュする。
3. 端末のプライベート IP アドレスと学内とを通信するためにサーバ内で KUINS-III に SNAT する。

また個別 VLAN 方式は下記の接続フローとなる。

1. 端末からのアクセスに対し、京都大学で発行申請された NII のクライアント証明書で認証するが、その CN には「全学アカウント@VLAN 管理番号」のように接続したい VLAN が指定されており、KUINS-DB に登録済みのアカウントであれば CN に紐付いた特定のプライベート IP アドレスを割り当てる。
2. 同様にルーティングをプッシュする。
3. 端末のプライベート IP アドレスを個別 VLAN の IP アドレスに SNAT する。どの VLAN の IP アドレスに SNAT するかは CN に紐付いた IP アドレスに設定されたポリシールーティングにより決められる。

4.2　サーバのシステム構成と各種設定

構築した OpenVPN サーバのシステム構成を表 4 に示す。全て CentOS8 標準または EPEL 拡張パッケージを用いて構成している。

サーバは仮想マシンで構築し KUINS-II、クライアント用 KUINS-III 及び各構内のメインスイッチにより QinQ に集約された研究室 VLAN を引き込み NIC に適切な IP アドレスを設定する。ここで仮の設定

表 4　OpenVPN サーバのシステム構成

機能	ソフトウェア名	バージョン
OS	Linux	4.18.0
VPN	openvpn	2.4.9
ネットワーク	NetworkManager	1.22.8
SNAT と転送	nftables	0.9.3
	firewalld	0.8.0

例を表 5 にまとめる。ens1 は KUINS-II のグローバルアドレスとして、ens2 はクライアント用 KUINS-III、VLAN 番号が付与された ens3 は個別 VLAN の KUINS-III アドレスとなっている。研究室 VLAN のルーティング名には VLAN 管理番号を使用する。また tun デバイスは OpenVPN にて自動的に割り当てられる。

表 5　ネットワークインターフェース例示

デバイス	IP アドレス	ゲートウェイ
ens1	192.0.2.1,192.0.2.2	192.0.2.254
ens2	172.16.0.252	172.16.0.254
ens3.1	172.16.1.252	172.16.1.254
ens3.2	172.16.2.252	172.16.2.254
:	:	:
tun0	10.1.0.1	-
tun1	10.2.0.1	-

デフォルトゲートウェイは KUINS-II のゲートウェイアドレスとしているが各 NIC のルーティングテーブルを設定 1 のように設定する。またポリシールーティングを設定 2 のように設定し、OpenVPN クライアント IP アドレスに応じたルーティングテーブルとなるように設定する。

設定 1　ルーティングテーブル

```
--/etc/sysconfig/network-scripts/route-ens1--
default via 192.0.2.254 dev ens1 table 200

--/etc/sysconfig/network-scripts/route-ens2--
default via 172.16.0.254 dev ens2 table 201

--/etc/sysconfig/network-scripts/route-ens3.1--
172.16.1.0/24 dev ens3.1 src 172.16.1.252 table 123456
default via 172.16.1.254 dev ens3.1 table 123456

--/etc/sysconfig/network-scripts/route-ens3.2--
172.16.2.0/24 dev ens3.2 src 172.16.2.252 table 123457
default via 172.16.2.254 dev ens3.2 table 123457
```

設定 2　ポリシールーティング

```
--/etc/sysconfig/network-scripts/rule-ens1--
from 192.0.2.0/24 table 200 priority 1

--/etc/sysconfig/network-scripts/rule-ens1--
from 10.1.0.0/21 table 201 priority 2

--/etc/sysconfig/network-scripts/rule-ens3.1--
from 10.2.0.5 table 123456 priority 3
from 10.2.0.6 table 123456 priority 4
from 10.2.0.7 table 123456 priority 5
 (KUINS-DBで申請されたアカウント数分を記載)

--/etc/sysconfig/network-scripts/rule-ens3.2--
from 10.2.0.8 table 123457 priority 6
```

また VPN クライアントからの通信が転送されるようにカーネルオプションの変更や nftables と firewalld

での通信許可設定を追加する。

同じく firewalld にて SNAT の設定も事前に設定しておく。設定 3 の最初の設定は共通 VLAN の端末用でそれ以降は個別 VLAN の端末用となっている。

設定 3　SNAT 設定

```
--/etc/firewalld/direct.xml--
<?xml version="1.0" encoding="utf-8"?>
<direct>
  <rule priority="0" table="nat" ipv="ipv4" chain="POSTROUTING"
        >-s 10.1.0.0/21 -o ens2 -j SNAT --to-source
        172.16.0.252</rule>
  <rule priority="0" table="nat" ipv="ipv4" chain="POSTROUTING"
        >-s 10.2.0.0/16 -o ens3.1 -j SNAT --to-source
        172.16.1.252</rule>
  <rule priority="0" table="nat" ipv="ipv4" chain="POSTROUTING"
        >-s 10.2.0.0/16 -o ens3.2 -j SNAT --to-source
        172.16.2.252</rule>
  :
</direct>
```

OpenVPN の共通 VLAN 方式を設定 4 に個別 VLAN 方式を設定 5 にまとめる。個別 VLAN 方式では IP アドレスやサーバ証明書や tun デバイス、ログファイルを変更している。また TLS 検証スクリプトの引数の変更とクライアントの設定ディレクトリを追加している。

設定 4　共通 VLAN 方式のサーバ設定

```
--/etc/openvpn/server/openvpn0.conf--
local 192.0.2.1
port 443
proto tcp-server
dev tun0

ca /etc/pki/tls/certs/ca.cer
crl-verify /etc/pki/tls/certs/fullcrlg4.crl
cert /etc/pki/tls/certs/server0.cer
key /etc/pki/tls/private/server0.key
dh /etc/pki/tls/private/dh2048.pem
script-security 2
tls-verify "/etc/openvpn/scripts/verify-cn-kuins.pl 0"
tls-version-min 1.2

topology subnet
server 10.1.0.0 255.255.248.0

push "dhcp-option DNS [DNS 1]"
push "dhcp-option DNS [DNS 2]"
push "redirect-gateway def1 bypass-dhcp"
keepalive 10 120
compress lz4-v2
push "compress lz4-v2"
max-clients 500
tcp-queue-limit 512
persist-key
persist-tun
log-append /var/log/openvpn/openvpn0.log
```

設定 5　個別 VLAN 方式のサーバ設定

```
--/etc/openvpn/server/openvpn1.conf--
local 192.0.2.2
port 443
proto tcp-server
dev tun1

ca /etc/pki/tls/certs/ca.cer
crl-verify /etc/pki/tls/certs/fullcrlg4.crl
cert /etc/pki/tls/certs/server1.cer
key /etc/pki/tls/private/server1.key
dh /etc/pki/tls/private/dh2048.pem
script-security 2
tls-verify "/etc/openvpn/scripts/verify-cn-kuins.pl 1"
tls-version-min 1.2

topology subnet
server 10.2.0.0 255.255.0.0
client-config-dir /etc/openvpn/server/ccd1

push "dhcp-option DNS [DNS 2]"
push "dhcp-option DNS [DNS 1]"
push "redirect-gateway def1 bypass-dhcp"
keepalive 10 120
compress lz4-v2
push "compress lz4-v2"
max-clients 500
tcp-queue-limit 512
persist-key
persist-tun
log-append /var/log/openvpn/openvpn1.log
```

TLS を検証する verify-cn-kuins.pl を設定 6 にまとめる。京都大学の発行申請証明書の確認に加えて、引数が 1 ならばクライアント設定ディレクトリに CN のファイルが存在するか確認する。

設定 6　verify-cn-kuins.pl

```
#!/usr/bin/perl
($server, $depth, $x509) = @ARGV;
if ($depth == 0) {
    if ($x509 !~ /O=Kyoto University,/ || $x509 !~ /OU=Kyoto
          University Integrated Information Network System,/) {
        exit 1;
    }
    if ($server == 1 && $x509 =~ / CN=([^,]+)/) {
        $cn = $1;
        if(! -e '/etc/openvpn/server/ccd1/'.$cn) {
            exit 1;
        }
    }
    exit 0;
}
exit 0;
```

また個別 VLAN 方式ではアカウント名とクライアント IP アドレスを紐付けるために設定 7 のように IP アドレスを記載した CN のファイルを配置する。

設定 7　クライアント設定ディレクトリ

```
--/etc/openvpn/server/ccd1/id1@123456--
ifconfig-push 10.2.0.5 255.255.0.0

--/etc/openvpn/server/ccd1/id2@123457--
ifconfig-push 10.2.0.8 255.255.0.0
```

5　システム運用予定

2020 年 10 月より個別 VLAN 接続機能を実装した OpenVPN サービスを試験サービスとして運用を開始している。IKEv2 が利用不可と連絡のあった利用者にはすでに連絡をしており、接続可能であった旨報告を受けている。今後 2020 年 12 月まで試験運用を継続し 2021 年 1 月から本サービス開始を予定している。

6　まとめ

- 既存 IKEv2 サービスが利用不可という利用者のために OpenVPN サービスにて不足していた個別 VLAN 接続サービス機能を実装した。
- 試験サービスとして運用を開始し利用者からは利用可となった旨報告があった。
- 運用コスト削減のため利用者数の少ない VPN サービスの廃止を予定しており、受け皿の OpenVPN サービスの機能強化は今後の VPN サービス運用面でも有用と考えている。

参考文献

[1] 大学 ICT 推進協議会 2016 年度年次大会
「京都大学における IKEv2 サービスの構築」 針木剛 2016 年

[2] 総合技術研究会 2017
「全学無線 LAN での研究室 VLAN 接続サービスの構築」 針木剛 2017 年