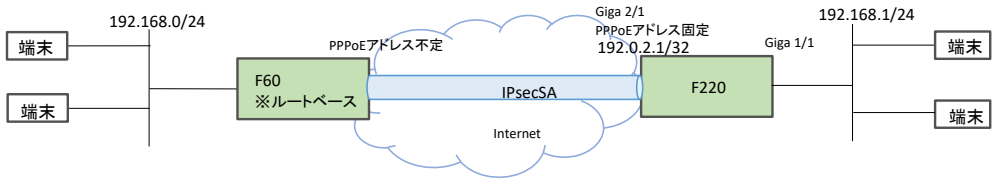
## 設定例

# F60とIPsecでトンネリングする：F60ルートベース-F220ルートベース

## 概要

F60をルートベース方式として（IPsecインタフェースを利用）、F220とIPsecトンネリング接続するための設定例です。
・暗号化対象(IPsecセレクタ)を全src/dstアドレスとして、双方で対向拠点のLANネットワークへのTunnel（IPsec）経路を登録すれば、SA接続および通信可能です。




## パラメータ設定例

ISAKMPポリシー

| | |
|---|---|
| IKEバージョン | 1 |
| モード | Aggressiveモード |
| 認証方式 | 事前共有鍵方式 |
| 暗号化方式 | AES 256ビット |
| ハッシュ方式 | SHA-1 |
| Diffie-Hellman | Group 14 |
| ライフタイム | 86400秒 |

IPSECポリシー

| | |
|---|---|
| PFS | Group 14 |
| 暗号化方式 | AES 256ビット |
| ハッシュ方式 | SHA-1 |
| ライフタイム | 28800秒 |
| フラグメント | ポストフラグメント |

## コマンド設定例

F60の設定

| | 設定例（F60） | 補足 |
|---|---|---|
| 1 | ip route 0.0.0.0 0.0.0.0 pppoe 1 | |
| 2 | ip route 192.168.1.0 255.255.255.0 connected ipsecif 1 | F220のLANネットワークへのTunnel（IPsec）経路を登録 |
| 3 | ip route 192.168.1.0 255.255.255.0 connected null 0 150 | IPsecインターフェースがダウンしたときに、F220のLANネットワーク宛の通信が平文で出力されないための設定<br>＃set security-association always-up設定により、SAの有無に連動してIPsecインタフェースがアップ、ダウンする |
| 4 | ! | |
| 5 | access-list 99 permit 192.168.0.0 0.0.0.255 | |
| 6 | ! | |
| 7 | vpn enable | |
| 8 | vpnlog enable | |
| 9 | ! | |
| 10 | ipsec access-list 1 ipsec ip any any | |
| 11 | ipsec access-list 64 bypass ip any any | |
| 12 | ipsec transform-set P2-POLICY esp-aes-256 esp-sha-hmac | |
| 13 | ! | |
| 14 | interface ipsecif 1 | |
| 15 | crypto map CENTER | |
| 16 | exit | |
| 17 | interface lan 1 | |
| 18 | ip address 192.168.0.254 255.255.255.0 | |
| 19 | exit | |
| 20 | interface pppoe 1 | |
| 21 | ip nat inside source list 99 interface | |
| 22 | pppoe server FLETS-ADSL | |
| 23 | pppoe account abc345@***.***.ne.jp zzzyyyxxx | |
| 24 | pppoe type host | |
| 25 | exit | |
| 26 | ! | |
| 27 | crypto isakmp policy 1 | |
| 28 | authentication prekey | |
| 29 | encryption aes 256 | |
| 30 | group 14 | |
| 31 | hash sha | |
| 32 | idtype-pre userfqdn | |
| 33 | key ascii SECRET-VPN | |
| 34 | lifetime 86400 | |
| 35 | my-identity id-kyoten | |
| 36 | negotiation-mode aggressive | |
| 37 | peer-identity address 192.0.2.1 | |
| 38 | exit | |
| 39 | crypto map CENTER 1 | |
| 40 | match address 1 | |
| 41 | set peer address 192.0.2.1 | |
| 42 | set pfs group14 | |
| 43 | set security-association lifetime seconds 28800 | |
| 44 | set security-association always-up | |
| 45 | set transform-set P2-POLICY | |
| 46 | exit | |
| 47 | ! | |
| 48 | end | |

F220の設定

| | 設定例（F220） | 補足 |
|---|---|---|
| 1 | access-list 100 permit udp any eq 500 192.0.2.1 0.0.0.0 eq 500 | VPNで使用するパケットを受信許可するフィルタリングの設定 |
| 2 | access-list 100 permit 50 any 192.0.2.1 0.0.0.0 | VPNで使用するパケットを受信許可するフィルタリングの設定 |
| 3 | access-list 111 deny ip any any | 学習フィルタリングの設定 |
| 4 | access-list 121 spi ip any any | 学習フィルタリングの設定 |
| 5 | ! | |
| 6 | ip route 0.0.0.0 0.0.0.0 tunnel 1 | |
| 7 | ip route 192.168.0.0 255.255.255.0 tunnel 2 | F60のLANネットワークへのTunnel（IPsec）経路を登録 |
| 8 | ip nat list 1 192.168.1.0 0.0.0.255 | |
| 9 | ! | |
| 10 | logging level informational | isakmpログを記録するためにログレベルを設定 |
| 11 | ! | |
| 12 | crypto ipsec policy P2-POLICY | IPsecポリシー設定（共有設定） |
| 13 | set pfs group14 | |
| 14 | set security-association lifetime seconds 28800 | |
| 15 | set security-association transform-keysize aes 256 256 256 | |
| 16 | set security-association transform esp-aes esp-sha-hmac | |
| 17 | set mtu 1454 | |
| 18 | set ip df-bit 0 | |
| 19 | set ip fragment post | |
| 20 | exit | |
| 21 | ! | |
| 22 | crypto ipsec selector SELECTOR | セレクタ設定（共有設定） |
| 23 | src 1 ipv4 any | 送信元セレクタを全IPv4アドレスを対象に設定 |
| 24 | dst 1 ipv4 any | 宛先セレクタを全IPv4アドレスを対象に設定 |
| 25 | exit | |
| 26 | ! | |
| 27 | crypto isakmp keepalive | |
| 28 | crypto isakmp log sa | |
| 29 | crypto isakmp log session | |
| 30 | crypto isakmp log negotiation-fail | |
| 31 | ! | |
| 32 | crypto isakmp policy P1-POLICY | ISAKMPポリシー設定（共有設定） |
| 33 | authentication pre-share | |
| 34 | encryption aes | |
| 35 | encryption-keysize aes 256 256 256 | |
| 36 | group 14 | |
| 37 | lifetime 86400 | |
| 38 | hash sha | |
| 39 | initiate-mode aggressive | |
| 40 | exit | |
| 41 | ! | |
| 42 | crypto isakmp profile PROF0001 | ISAKMPプロファイル設定（対向拠点毎に設定） |
| 43 | match identity user id-kyoten | |
| 44 | local-address 192.0.2.1 | |
| 45 | set isakmp-policy P1-POLICY | |
| 46 | set ipsec-policy P2-POLICY | |
| 47 | ike-version 1 | |
| 48 | local-key SECRET-VPN | |
| 49 | exit | |
| 50 | ! | |
| 51 | crypto map KYOTEN0001 ipsec-isakmp | CRYPTO MAP設定（対向拠点毎に設定） |
| 52 | match address SELECTOR | |
| 53 | set isakmp-profile PROF0001 | |
| 54 | exit | |
| 55 | ! | |
| 56 | interface GigaEthernet 1/1 | |
| 57 | vlan-id 1 | |
| 58 | bridge-group 1 | |
| 59 | channel-group 1 | |
| 60 | exit | |
| 61 | ! | |
| 62 | interface GigaEthernet 2/1 | |
| 63 | vlan-id 2 | |
| 64 | bridge-group 2 | |
| 65 | pppoe enable | |
| 66 | exit | |
| 67 | ! | |
| 68 | interface Port-channel 1 | |
| 69 | ip address 192.168.1.254 255.255.255.0 | |
| 70 | mss 1300 | |
| 71 | exit | |
| 72 | ! | |
| 73 | interface Tunnel 1 | |
| 74 | description FLETS | |
| 75 | ip address 192.0.2.1 255.255.255.255 | |
| 76 | ip access-group 100 in | |
| 77 | ip access-group 111 in | |
| 78 | ip access-group 121 out | |
| 79 | ip nat inside source list 1 interface | |
| 80 | tunnel mode pppoe profile PPPOE_PROF | |
| 81 | pppoe interface gigaethernet 2/1 | |
| 82 | exit | |
| 83 | ! | |
| 84 | interface Tunnel 2 | Tunnel（IPsec）インタフェース設定（対向拠点毎に設定） |
| 85 | tunnel mode ipsec map KYOTEN0001 | |
| 86 | exit | |
| 87 | ! | |
| 88 | pppoe profile PPPOE_PROF | |
| 89 | account abc012@***.***.ne.jp xxxyyyzzz | |
| 90 | exit | |
| 91 | ! | |
| 92 | end | |