# L2TP/IPsecを利用するための設定例

## 対象装置：FITELnet F70/F71/F220/F221/F220 EX/F221 EX

Phase1 SA：RSA認証、PPPセッション：Local認証

※ログインID/Passwordは"test"/"test"です。

| | 設定例 | 補足 |
|---|---|---|
| 1 | access-list 100 permit udp any host <FITELnet_global_IPaddress> eq 500 | フィルタ用(許可　isakampパケット) |
| 2 | access-list 100 permit udp any host <FITELnet_global_IPaddress> eq 4500 | フィルタ用(許可　sakampパケット NAT-T) |
| 3 | access-list 100 permit 50 any any | フィルタ用(許可　ESPパケット) |
| 4 | access-list 111 deny ip any any | フィルタ用（拒否） |
| 5 | access-list 121 spi ip any any | フィルタ用（SPI 登録） |
| 6 | ! | |
| 7 | ip route 0.0.0.0 0.0.0.0 tunnel 1 | 経路設定 |
| 8 | ip local pool POOL1 192.168.1.101 192.168.1.200 | IPsec やL2TP/PPP により通知するアドレス範囲の設定 |
| 9 | ip nat list 1 192.168.1.0 0.0.0.255 | NAT/NAT+ 変換で変換後アドレスとして利用可能範囲の設定 |
| 10 | ! | |
| 11 | traffic-manager network | |
| 12 | to-host protocol ipv4 l2tp policer 11 | 自局宛トラフィックが入力されるポリサーの設定 |
| 13 | exit | |
| 14 | ! | |
| 15 | hardware-fault-detection action reboot | ハードウェア故障を検出した際の動作を指定( 装置再起動 ) |
| 16 | ! | |
| 17 | logging buffer level informational | 装置内部バッファへ出力するログレベルを指定<br>※"show logging buffer"で確認可能 |
| 18 | ! | |
| 19 | aaa authentication login default local | ログイン認証方式を指定<br>local: usernameコマンドで設定した内容( id, password )で認証<br>login: "password login"コマンドで設定した内容( id: operator )<br>※default設定 |
| 20 | aaa authentication ppp LOCAL_AUTH local-group LOCAL_GROUP | PPP セッションの認証方式を設定 |
| 21 | aaa authorization exec default local | TELNETログイン時の許可方式を指定<br>local: usernameコマンドで設定した特権レベルでログイン許可 |
| 22 | ! | |
| 23 | aaa local group LOCAL_GROUP | CLIENT- データベース設定モード |
| 24 | username user1 password secret1 | 接続を許可するユーザ名とパスワードの設定 |
| 25 | username user2 password secret2 | |
| 26 | exit | |
| 27 | ! | |
| 28 | username test privilege 15 password 2 $1$KcitZI/P$j4UYIma9EHAyPjTWQwyO50 | ユーザ名、パスワード、ログイン時の特権レベルを指定<br>※例はid: test / password: test<br>※以下の設定が有る場合に有効<br>aaa authorization exec default local<br>aaa authentication login default local ※Telnetログイン用<br>line console<br>authorization exec default local ※Consoleログイン用<br>exit |
| 29 | ! | |
| 30 | hostname FITELnet | hostname設定 |
| 31 | ! | |
| 32 | crypto ipsec policy IPSECPOL_1 | IPsecポリシー設定( Phase2 SAのパラメータを指定 ) |
| 33 | mode transport | |
| 34 | set security-association lifetime seconds 86400 | Phase2 SAのLifetime(秒)を指定<br>※defaultのRekeyの開始タイミングはResponder動作時はLifetime満了の30秒前、Initiator動作時は90秒前に開始<br>set security-association softlimit initiate seconds 90<br>set security-association softlimit respond seconds 30 |
| 35 | set security-association transform-keysize aes 128 256 256 | 暗号化アルゴリズム( AES )の鍵サイズを指定<br>※受け入れ可能な鍵サイズの最小値、最大値、Initiator提案時の最優先値 |
| 36 | set security-association transform esp-aes esp-3des esp-md5-hmac esp-sha-hmac | 暗号化アルゴリズム( AES )とハッシュアルゴリズム( SHA1 )を指定 |
| 37 | set ip df-bit 0 | ポストフラグメント指定 ※プリフラグメント指定の場合は削除<br>※暗号化後のESPパケットのDFビットを"0"に設定します。<br>( defaultでは暗号化対象パケットのDFビットをコピーします ) |
| 38 | set ip fragment post | ポストフラグメント指定 ※プリフラグメント指定の場合は削除 |
| 39 | set udp-encapsulation nat-t keepalive interval 30 always-send | ESP パケットのUDP カプセル化を行うポリシー個別の方式の設定 |
| 40 | exit | |
| 41 | ! | |
| 42 | crypto isakmp keepalive always-send | DPD設定( Traffic監視 )<br>※interval内にESP、又はDPD-R-U-THEREパケットを受信していない場合にRequestを送信します。<br>( interval毎に毎回送信する場合はalways-sendを指定 ) |
| 43 | crypto isakmp log sa detail | SYSLOGにSA確立／解放のログを出力<br>※Phase1, 2 SA確立時にSession確立、どちらも削除された際にSession切断となります |
| 44 | crypto isakmp log session detail | SYSLOGにSession確立・切断のログを出力<br>※Phase1, 2 SA確立時にSession確立、どちらも削除された際にSession切断となります |
| 45 | crypto isakmp log negotiation-fail detail | SYSLOGにIKEネゴシエーション失敗のログを出力 |
| 46 | ! | |

| | 設定例 | 補足 |
|---|---|---|
| 47 | crypto isakmp policy ISAPOL_1 | ISAKMPポリシー設定( Phase1 SAのパラメータを指定 ) |
| 48 | authentication rsa-sig | RSA-signatures認証を指定 |
| 49 | encryption aes | 暗号化アルゴリズムを指定 |
| 50 | encryption-keysize aes 256 256 256 | 暗号化アルゴリズム( AES )の鍵サイズを指定<br>※受け入れ可能な鍵サイズの最小値、最大値、Initiator提案時の最優先値 |
| 51 | group 1 2 5 14 15 | DHグループを指定 |
| 52 | lifetime 86400 | Phase1 SAのLifetime(秒)を指定<br>※Lifetime満了時にISAKMP SAを削除し、Rekey、及びDPD契機で再接続します |
| 53 | hash sha | ハッシュアルゴリズムを指定 |
| 54 | initiate-mode main | IKE接続方式としてMainモードを指定 |
| 55 | exit | |
| 56 | ! | |
| 57 | crypto isakmp profile ISAPROF_001 | ISAKMPプロファイル設定 |
| 58 | self-identity fqdn CENTER.example.com | 本装置の識別方法を設定( fqdn="CENTER.example.com" )<br>※証明書登録のために必要な設定です。 |
| 59 | set isakmp-policy ISAPOL_1 | ISAKMPポリシーを指定 |
| 60 | set ipsec-policy IPSECPOL_1 | IPsecポリシーを指定 |
| 61 | ike-version 1 | IKEバージョンを指定 |
| 62 | ca trustpoint rootCA | 登録したCA証明書名を指定( rootCA ) |
| 63 | exit | |
| 64 | ! | |
| 65 | crypto map MAP_001 ipsec-isakmp dynamic | CRYPTO MAP設定 |
| 66 | set isakmp-profile ISAPROF_001 | セレクタを指定 |
| 67 | exit | ISAKMPプロファイルと紐付け |
| 68 | ! | |
| 69 | interface GigaEthernet 1/1 | 物理インタフェース |
| 70 | vlan-id 1 | VLAN指定( ポートVLAN ) ※必須 |
| 71 | bridge-group 1 | bridge-group指定 ※必須 |
| 72 | channel-group 1 | 論理インタフェース( Port-channel )と紐付け |
| 73 | exit | |
| 74 | ! | |
| 75 | interface GigaEthernet 2/1 | 物理インタフェース |
| 76 | vlan-id 2 | VLAN指定( ポートVLAN ) ※必須 |
| 77 | bridge-group 2 | bridge-group指定 ※必須 |
| 78 | pppoe enable | pppoe enable |
| 79 | exit | |
| 80 | ! | |
| 81 | interface Port-channel 1 | 論理インタフェース設定 |
| 82 | ip address 192.168.1.1 255.255.255.0 | アドレス設定 |
| 83 | ip proxy-arp | proxy-arp 動作を行う設定 |
| 84 | exit | |
| 85 | ! | |
| 86 | interface Tunnel 1 | Tunnelインタフェース設定( PPPoE Tunnel ) |
| 87 | ip address <FITELnet_global_IPaddress> 255.255.255.255 | アドレス設定 |
| 88 | ip access-group 100 in | フィルタリング設定 |
| 89 | ip access-group 111 in | フィルタリング設定 |
| 90 | ip access-group 121 out | フィルタリング設定 |
| 91 | ip nat inside source list 1 interface | nat設定 |
| 92 | tunnel mode pppoe profile PPPOE_PROF | PPPoEプロファイルと紐付け |
| 93 | pppoe interface gigaethernet 2/1 | PPPoEインタフェース指定 |
| 94 | exit | |
| 95 | ! | |
| 96 | ppp-template PPP_001 | PPP テンプレート設定モード |
| 97 | pool POOL1 | PPP で通知するIP アドレス範囲の、アドレスプール名を設定 |
| 98 | ppp authentication chap LOCAL_AUTH | PPP の認証タイプと認証方式名を設定 |
| 99 | exit | |
| 100 | ! | |
| 101 | l2tpv2 tunnel-profile LNS_001 | L2TPv2 トンネル設定モード |
| 102 | ppp accept template PPP_001 | 該当L2TPv2 トンネル上で収容するPPP セッションを関連付け |
| 103 | local name LNS1 | LNS装置のホスト名を指定 |
| 104 | tunnel protection ipsec map MAP_001 | VPN セレクタ名指定 |
| 105 | exit | |
| 106 | ! | |
| 107 | l2tpv2 log ccn | L2TPv2 メッセージを出力（Control connection の確立/ 解放） |
| 108 | l2tpv2 log session | L2TPv2 メッセージを出力（セッション確立/ 解放） |
| 109 | l2tpv2 log negotiation-fail | L2TPv2 メッセージを出力（ネゴシエーション失敗） |
| 110 | ! | |
| 111 | pppoe profile PPPOE_PROF | PPPoEプロファイル |
| 112 | account <pppoe_user> <pppoe_password> | アカウント設定 |
| 113 | exit | |
| 114 | ! | |
| 115 | dns-server ip enable | DNS サーバ機能およびProxyDNS機能の有効化 |
| 116 | ! | |
| 117 | proxydns domain 1 any * any ipcp tunnel 1 | ProxyDNSの正引き動作条件の設定 |
| 118 | ! | クラスにマッチしたパケット数をカウントする設定 |
| 119 | end | クラスにマッチしたパケットを経路表に従って送信する設定 |