固定IPサービスで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

※下記の設定を、VNE各社の固定IP設定例に追加してご使用ください。
※ログインID/Passwordは"test"/"test"です。

	設定例	補足
1	access-list 100 permit udp any host ##固定IPv4グローバルアドレス## eq 500	IPv4アクセスリスト（ IKE ）
2	access-list 100 permit udp any host ##固定IPv4グローバルアドレス## eq 4500	IPv4アクセスリスト（ IKE NAT-T ）
3	access-list 100 permit 50 any host ##固定IPv4グローバルアドレス##	IPv4アクセスリスト（ ESP ）
4	access-list 4000 permit 4 ##トンネル終端装置 IPv6アドレス##/128 any	IPv6アクセスリスト（ v4/v6 IPinIP ）
5	!	
6	ip local pool POOL1 192.168.0.129 192.168.0.254	PPPのIPCPによる払い出しアドレス設定
7	!	
8	ip dhcp server-profile LAN	
9	address 192.168.0.4 192.168.0.128	DHCP払い出しアドレス設定
10	exit	
11	!	
12	ipinip tunnel-profile IPIP1	IPinIPトンネルプロファイル
13	set mss 1234	MSS設定（ L2TP/IPsecのinner MTUに合わせた値です。）
14	exit	
15	!	
16	aaa authentication ppp PPP_AUTH1 local-group LOCAL_AUTH1	PPPの認証方式（ 装置内データベースによる認証/RADIUS ）
17	!	
18	aaa local group LOCAL_AUTH1	装置内データベース設定 ※"aaa authentication ppp PPP_AUTH1 local-group LOCAL_AUTH1"と紐付け
19	username user1 password pass1	PPPアカウント・パスワード設定
20	username user1 interface tunnel 1001	PPPアカウントとL2TPv2トンネルインタフェースを紐付け ※Dynamicにトンネルインタフェースを割り当てる場合は不要（ interface Tunnelの設定も不要 ）
21	username user2 password pass2	PPPアカウント・パスワード設定
22	username user2 interface tunnel 1002	PPPアカウントとL2TPv2トンネルインタフェースを紐付け ※Dynamicにトンネルインタフェースを割り当てる場合は不要（ interface Tunnelの設定も不要 ）
23	exit	
24	!	
25	crypto ipsec udp-encapsulation nat-t keepalive interval 60 always-send	NAT-T有効化
26	!	
27	crypto ipsec policy IPsec_POLICY	IPsecポリシー設定（ Phase2 SAのパラメータを指定 ）
28	mode transport	トランスポートモード指定 ※L2TP/IPsecでは必須
29	set security-association lifetime seconds 3600	Lifetime(秒)を指定
30	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 ※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
31	set security-association transform esp-aes esp-3des esp-md5-hmac esp-sha-hmac	暗号化アルゴリズム・ハッシュアルゴリズム指定
32	set ip df-bit 0	IPsec OuterのDFビットを0にします。※L2TP/IPsecでは必須
33	set ip fragment post	IPsecのフラグメント方式を指定 ※L2TP/IPsecでは必須
34	exit	
35	!	
36	crypto isakmp log sa	SYSLOGにSA確立・切断のログを出力
37	crypto isakmp log session	SYSLOGにSession確立・切断のログを出力 ※Phase1, 2 SA両方確立時にSession確立、どちらも削除された際にSession切断となります
38	crypto isakmp log negotiation-fail	SYSLOGにIKEネゴシエーション失敗のログを出力
39	!	
40	crypto isakmp policy ISAKMP_POLICY	ISAKMPポリシー設定（ Phase1 SAのパラメータを指定 ）
41	authentication pre-share	Pre-shared Key認証を指定
42	encryption aes	暗号化アルゴリズムを指定
43	encryption-keysize aes 128 256 256	暗号化アルゴリズムの鍵サイズを指定 ※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
44	group 1 2 5 14 15	DHグループを指定
45	lifetime 3600	Lifetime(秒)を指定
46	hash sha sha-256	ハッシュアルゴリズムを指定
47	initiate-mode main	Mainモードを指定
48	exit	
49	!	
50	crypto isakmp profile PROF1	ISAKMPプロファイル設定
51	local-address source-interface tunnel 1	IPsecトンネル終端アドレス指定
52	set isakmp-policy ISAKMP_POLICY	ISAKMPポリシーを指定
53	set ipsec-policy IPsec_POLICY	IPsecポリシーを指定
54	ike-version 1	IKEバージョンを指定
55	local-key secret	Pre-shared Keyを指定
56	exit	
57	!	
58	crypto map MAP1 ipsec-isakmp dynamic	CRYPTO MAP設定
59	set isakmp-profile PROF1	ISAKMPプロファイルと紐付け
60	exit	
61	!	

	設定例	補足
62	interface Port-channel 11	
63	ip proxy-arp	プロキシARP設定
64	mss 1234	MSS設定 （ L2TP/IPsecのinner MTUに合わせた値です。）
65	link-state always-up	物理インタフェースがダウンしている状態でもPort-channelを アップした状態にします。
66	exit	
67	!	
68	interface Tunnel 1	
69	ip access-group 100 in	IPv4アクセスリスト紐づけ(IKE)
70	exit	
71	!	
72	interface Tunnel 1001	L2TPv2トンネルインタフェース設定
73	tunnel mode l2tpv2	L2TPv2モード指定
74	exit	
75	!	
76	interface Tunnel 1002	L2TPv2トンネルインタフェース設定
77	tunnel mode l2tpv2	L2TPv2モード指定
78	exit	
79	!	
80	ppp-template PPP_TEMP1	PPPテンプレート設定
81	pool POOL1	PPP払い出しアドレス用プール指定
82	ppp authentication chap PPP_AUTH1	PPP認証タイプ(PAP/CHAP/MS-CHAPv2/CHAP-PAP)・ 認証方式(ローカルデータベース/RADIUS)指定 ※"aaa authentication ppp PPP_AUTH1 local-group LOCAL_AUTH1"と紐付け
83	dns 192.168.0.2 192.168.0.3	DNSアドレス指定 ※IPoE上のL2TP/IPsec Tunnelに対して自出しパケットを 送信する事が出来ないため、本装置のアドレスを指定する事は出来ません （2021年6月本制限解除予定）。
84	exit	
85	!	
86	l2tpv2 tunnel-profile LNS1	L2TPv2トンネル設定
87	ppp accept template PPP_TEMP1	PPPテンプレート設定と紐付け
88	local name LNS1	LNSホスト名設定
89	tunnel protection ipsec map MAP1	IPsec(CRYPTO MAP)と紐付け
90	exit	
91	!	
92	l2tpv2 log ccn	SYSLOGにL2TPv2 Control connection確立・切断のログを出力
93	l2tpv2 log session	SYSLOGにL2TPv2 Session確立・切断のログを出力
94	l2tpv2 log negotiation-fail	SYSLOGにL2TPv2ネゴシエーション失敗のログを出力
95	!	
96	end	