固定IPサービスでL2TPv3/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	bridge-group 1001	ブリッジグループ設定
7	bridge ip adjust-mss 1312	L2 MSS書き換え
8	exit	
9	!	
10	bridge-group 1002	ブリッジグループ設定
11	bridge ip adjust-mss 1312	L2 MSS書き換え
12	exit	
13	!	
14	crypto ipsec udp-encapsulation nat-t keepalive interval 60 always-send	NAT-T有効化
15	!	
16	crypto ipsec policy IPsec_POLICY	IPsecポリシー設定（ Phase2 SAのパラメータを指定 ）
17	set security-association lifetime seconds 28800	Lifetime(秒)を指定
18	set security-association transform-keysize aes 256 256 256	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
19	set security-association transform esp-aes esp-sha-hmac	暗号化アルゴリズム・ハッシュアルゴリズム指定
20	set mtu 1460	MTU設定 ※ESPカプセル化後のサイズを指定
21	exit	
22	!	
23	crypto ipsec selector SELECTOR	セレクタ設定
24	src 1 ipv4 any	送信元セレクタ(v4)を指定
25	dst 1 ipv4 any	宛先セレクタ(v4)を指定
26	exit	
27	!	
28	crypto isakmp log sa	SYSLOGにSA確立・切断のログを出力
29	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
30	crypto isakmp log negotiation-fail	SYSLOGにIKEネゴシエーション失敗のログを出力
31	crypto isakmp negotiation retry timer 10 limit 2 timer-max 30 guard-time 0	IKEネゴシエーションの再送設定 ※設定はデフォルト値 再送間隔：10秒 / 再送回数：2回 / 最大再送間隔：30秒 / 再送ガード時間：0秒 => 最大再送間隔になるまで再送毎に再送間隔が2倍になるため、初回送信から10秒後に再送1回目、20秒後に再送2回目、30秒後にタイムアウトとなります。 ※再送ガード時間を指定した場合、ネゴパケット送信から再送ガード時間内に受信した再送パケットを破棄します。
32	!	
33	crypto isakmp policy ISAKMP_POLICY	ISAKMPポリシー設定（ Phase1 SAのパラメータを指定 ）
34	authentication pre-share	Pre-shared Key認証を指定
35	encryption aes	暗号化アルゴリズムを指定
36	encryption-keysize aes 256 256 256	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
37	group 5	DHグループを指定
38	lifetime 86400	Lifetime(秒)を指定
39	hash sha	ハッシュアルゴリズムを指定
40	initiate-mode aggressive	Aggressiveモードで接続（ Mainモードの場合は"initiate-mode main" ）
41	exit	
42	!	
43	crypto isakmp profile PROF1	ISAKMPプロファイル設定
44	match identity host test1.example.com	リモート側のIKE ID（ FQDN ）を指定
45	local-address ##固定IPv4グローバルアドレス##	IPsecトンネル終端アドレス指定
46	self-identity address ##固定IPv4グローバルアドレス##	ローカル側のIKE ID（ IPv4 ）を指定
47	set isakmp-policy ISAKMP_POLICY	ISAKMPポリシーを指定
48	set ipsec-policy IPsec_POLICY	IPsecポリシーを指定
49	ike-version 1	IKEバージョンを指定
50	local-key secret1	Pre-shared Keyを指定
51	exit	
52	!	
53	crypto isakmp profile PROF2	ISAKMPプロファイル設定
54	match identity host test2.example.com	リモート側のIKE ID（ FQDN ）を指定
55	local-address ##固定IPv4グローバルアドレス##	IPsecトンネル終端アドレス指定
56	self-identity address ##固定IPv4グローバルアドレス##	ローカル側のIKE ID（ IPv4 ）を指定
57	set isakmp-policy ISAKMP_POLICY	ISAKMPポリシーを指定
58	set ipsec-policy IPsec_POLICY	IPsecポリシーを指定
59	ike-version 1	IKEバージョンを指定
60	local-key secret2	Pre-shared Keyを指定
61	exit	

	設定例	補足
62	!	
63	crypto session release ipsec-lost-time 5	IPsec SAが無い状態が指定した時間継続した場合にISAKMP SAを削除し、セッションを切断します。
64	!	
65	crypto map MAP1 ipsec-isakmp	CRYPTO MAP設定
66	match address SELECTOR	セレクタ指定
67	set isakmp-profile PROF1	ISAKMPプロファイルと紐付け
68	exit	
69	!	
70	crypto map MAP2 ipsec-isakmp	CRYPTO MAP設定
71	match address SELECTOR	セレクタ指定
72	set isakmp-profile PROF2	ISAKMPプロファイルと紐付け
73	exit	
74	!	
75	interface GigaEthernet 1/3.1001	サブインタフェース設定
76	vlan-id 1001	VLANタグ設定
77	bridge-group 1001	ブリッジグループ設定
78	exit	
79	!	
80	interface GigaEthernet 1/3.1002	サブインタフェース設定
81	vlan-id 1002	VLANタグ設定
82	bridge-group 1002	ブリッジグループ設定
83	exit	
84	!	
85	interface Loopback 1	Loopbackインタフェース設定
86	ip address 192.168.1.1	L2TPv3終端アドレス設定
87	exit	
88	!	
89	interface Port-channel 11	
90	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。
91	exit	
92	!	
93	interface Tunnel 1	
94	ip access-group 100 in	IPv4アクセスリスト紐づけ(IKE, ESP)
95	exit	
96	!	
97	interface Tunnel 101	IPsecトンネルインタフェース設定
98	tunnel mode ipsec map MAP1	トンネルモード指定"CRYPTO MAP設定"と紐付け
99	link-state sync-sa	SA確立時にTunnelインタフェースをアップさせます。
100	exit	
101	!	
102	interface Tunnel 102	IPsecトンネルインタフェース設定
103	tunnel mode ipsec map MAP2	トンネルモード指定"CRYPTO MAP設定"と紐付け
104	link-state sync-sa	SA確立時にTunnelインタフェースをアップさせます。
105	exit	
106	!	
107	interface Tunnel 1001	L2TPv3トンネルインタフェース設定
108	tunnel mode l2tpv3 pseudowire PW1	トンネルモード指定"L2TPv3 Pseudowire設定"と紐付け
109	bridge-group 1001	ブリッジグループ指定 ※Tunnel間の折り返しを抑制する場合は"client"オプションを指定 "client"オプションを指定した場合、別の"client"指定したインタフェース間の中継は行いません。(default : server)
110	exit	
111	!	
112	interface Tunnel 1002	L2TPv3トンネルインタフェース設定
113	tunnel mode l2tpv3 pseudowire PW2	トンネルモード指定"L2TPv3 Pseudowire設定"と紐付け
114	bridge-group 1002	ブリッジグループ指定 ※Tunnel間の折り返しを抑制する場合は"client"オプションを指定 "client"オプションを指定した場合、別の"client"指定したインタフェース間の中継は行いません。(default : server)
115	exit	
116	!	
117	l2tpv3 log ccn	SYSLOGにL2TPv3のControl connection確立/解放のログを記録
118	l2tpv3 log session	SYSLOGにL2TPv3セッション確立・切断時のログを記録
119	l2tpv3 log negotiation-fail	SYSLOGにL2TPv3ネゴ失敗時のログを記録
120	l2tpv3 retransmit retries 2	L2TPv3メッセージ再送時の再送回数を指定(default : 再送回数は10回で動作します)
121	l2tpv3 retransmit timer 5 timer-max 10	L2TPv3 メッセージ再送時の再送間隔を指定 ＊再送毎に再送間隔が2倍になります (最大再送間隔以上になる場合は最大再送間隔で送信します) (default : 再送間隔は1秒、最大再送間隔は8秒で動作します)
122	l2tpv3 hello interval 30	helloパケットの送信間隔(秒)指定
123	!	
124	l2tpv3 tunnel-profile PF1	L2TPv3プロファイル設定
125	mode l2tpv3	L2TPv3モード指定 l2tpv3 : RFC3931準拠 l2tpv3ext : cisco 独自モード udp : UDPモード
126	tunnel source 192.168.1.1	Local側のL2TPv3終端アドレスを指定
127	tunnel protection ipsec tunnel 101	IPsec Tunnelインタフェースを指定
128	hostname local FITELnet	Local側から送信する"Host Name AVP"に含むホスト名を指定
129	exit	
130	!	

	設定例	補足
131	l2tpv3 tunnel-profile PF2	L2TPv3プロファイル設定
132	mode l2tpv3	L2TPv3モード指定 l2tpv3　：RFC3931準拠 l2tpv3ext：cisco 独自モード udp　　：UDPモード
133	tunnel source 192.168.1.1	Local側のL2TPv3終端アドレスを指定
134	tunnel protection ipsec tunnel 102	IPsec Tunnelインタフェースを指定
135	hostname local FITELnet	Local側から送信する"Host Name AVP"に含むホスト名を指定
136	exit	
137	!	
138	l2tpv3 pseudowire PW1	L2TPv3 Pseudowire設定
139	set profile PF1	L2TPv3プロファイルを指定
140	set mtu 1390	MTU設定※L2TPv3カプセル化後のサイズを指定
141	remote-end-id ascii test1	Remote側から受信する"Remote End ID AVP"に含まれるセッション識別用のIDを指定
142	exit	
143	!	
144	l2tpv3 pseudowire PW2	L2TPv3 Pseudowire設定
145	set profile PF2	L2TPv3プロファイルを指定
146	set mtu 1390	MTU設定※L2TPv3カプセル化後のサイズを指定
147	remote-end-id ascii test2	Remote側から受信する"Remote End ID AVP"に含まれるセッション識別用のIDを指定
148	exit	
149	!	
150	end	