対象装置：FITELnet F2500

	EAP-MSCHAPv2 Local認証 設定例	補足
1	access-list 111 permit udp any host 10.0.0.1 eq 500	
2	access-list 111 permit udp any host 10.0.0.1 eq 4500	
3	access-list 111 permit icmp any host 10.0.0.1	
4	access-list 111 permit 50 any host 10.0.0.1	
5	access-list 121 spi ip any any	
6	!	
7	ip route 0.0.0.0 0.0.0.0 10.0.0.2	
8	ip route vrf VRF1 0.0.0.0 0.0.0.0 192.168.0.254	
9	ip route 192.168.1.0 255.255.255.0 null 0	払い出しアドレスを包含するnull経路(/24) ※払い出しアドレスを包含するStatic経路(/24)をデフォルトゲートウェイに設定する前提(ループ防止) ※SA確立時に払い出されるアドレス宛て以外のパケットを廃棄します。
10	ip local pool POOL1 192.168.1.1 192.168.1.254	アドレスプール設定 ※Configuration Payloadによる払い出しアドレスのレンジを指定
11	!	
12	ip vrf VRF1	VRF定義
13	rd 1:1	RD値を指定
14	exit	
15	!	
16	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 ※"show logging buffer"で確認可能 ※IPsecのログを出力する場合は"informational"を指定
17	!	
18	aaa authentication ike-client AUTH1 local-group LOCAL1	拡張認証方法を指定(Local認証)
19	aaa authorization network CP1 local-group CONFIG1	アドレス払い出し方法を指定
20	!	
21	aaa local group LOCAL1	拡張認証用ローカルデータベース設定
22	username user1 password pass1	EAPのID/Passwordを指定
23	username user2 password pass2	
24	exit	
25	!	
26	ntp server A.B.C.D	NTPサーバと時刻同期する設定 ★お客様の環境に合わせて設定お願いします。本装置はVRFのインタフェースでは時刻同期できませんので、ご注意ください。
27	!	
28	hostname IPsecGW	hostname指定
29	!	
30	crypto ipsec udp-encapsulation nat-t keepalive interval 60	NAT-T有効化
31	!	
32	crypto ipsec policy IPsec_POLICY	IPsecポリシー設定(Phase2 SAのパラメータを指定)
33	set security-association lifetime seconds 3600	Lifetime(秒)を指定
34	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
35	set security-association transform esp-aes esp-sha-hmac esp-sha256-hmac	暗号化アルゴリズム(AES)とハッシュアルゴリズム(SHA1,SHA256)を指定
36	set mtu 1500	暗号化後のMTU値を指定(default: 1500 Bytes) ★お客様の環境に合わせて設定お願いします。
37	set mss 1360	MSS値を指定　★お客様の環境に合わせて設定お願いします。
38	set ip df-bit 0	ESPパケットのDFビットを"0"に設定
39	set ip fragment post	ポストフラグメント指定
40	sa-up route	SA-UP経路設定 ※Configuration Payloadによる払い出しアドレス宛ての経路を登録します。
41	exit	
42	!	
43	crypto ipsec selector SELECTOR	セレクタ設定
44	src 1 ipv4 any	送信元セレクタ(v4)を指定
45	src 2 ipv6 any	送信元セレクタ(v6)を指定
46	dst 1 ipv4 any	宛先セレクタ(v4)を指定
47	dst 2 ipv6 any	宛先セレクタ(v6)を指定
48	exit	
49	!	
50	crypto isakmp keepalive interval 30	通信が無い場合に、DPDメッセージを30秒間隔で送信
51	crypto isakmp log sa detail	SYSLOGにSA確立・切断のログを出力
52	crypto isakmp log session detail	SYSLOGにSession確立・切断のログを出力 ※IKE SA, CHILD 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
53	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
54	!	
55	crypto isakmp client configuration group CONFIG1	Configuration Payloadによる払い出し設定
56	pool POOL1	アドレスプール指定
57	exit	
58	!	
59	crypto isakmp policy ISAKMP_POLICY	ISAKMPポリシー設定(Phase1 SAのパラメータを指定)
60	authentication rsa-sig	RSA認証を指定
61	encryption aes	暗号化アルゴリズムを指定(AES)
62	encryption-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
63	group 2 5 14 15	DHグループを指定(2, 5, 14, 15)
64	lifetime 86400	Lifetime(秒)を指定
65	hash sha sha-256 sha-384 sha-512	ハッシュアルゴリズムを指定(SHA1, SHA2-256, 384, 512)
66	exit	
67	!	

	EAP-MSCHAPv2 Local認証 設定例	補足
68	crypto isakmp profile PROF1	ISAKMPプロファイル設定
69	local-address 10.0.0.1	ローカル側のIPsec終端アドレスを指定
70	self-identity fqdn IPsecGW.example.com	ローカル側のIKE IDを指定(FQDN) 自装置の証明書に含まれる"Subject Alternative Name"と一致している必要があります。 ※Windows端末と接続する場合は"Common Name"とも一致させて下さい。
71	set isakmp-policy ISAKMP_POLICY	ISAKMPポリシーを指定
72	set ipsec-policy IPsec_POLICY	IPsecポリシーを指定
73	ca trustpoint CA1	CA証明書名を指定
74	client authentication list AUTH1	拡張認証方法を指定
75	client authentication type eap-mschapv2	認証方式にEAP MS-CHAPv2を指定
76	client authentication eap-identity request	認証時にEAP IDを要求
77	client configuration address respond	Configuration Payloadによるアドレス払い出し方法を指定(Request/Reply方式)
78	isakmp authorization list CP1	Configuration Payloadによる払い出し情報を指定
79	pki revocation-check none	証明書失効リストチェックの無効化 ※CRLを取得する場合は"crl"、または"crl none"を指定して下さい。
80	exit	
81	!	
82	crypto session identification address	リモート側のIPアドレスでセッションを識別します。
83	!	
84	crypto map MAP1 ipsec-isakmp dynamic	CRYPTOマップ設定
85	match address SELECTOR	セレクタを指定
86	set isakmp-profile PROF1	ISAKMPプロファイルと紐付け
87	vrf VRF1	VRFを指定 ※暗号化対象が属すVRFを指定します。
88	exit	
89	!	
90	interface GigaEthernet 1/1	
91	ip access-group 111 in	
92	ip access-group 121 out	
93	channel-group 1	
94	exit	
95	!	
96	interface GigaEthernet 1/2	
97	channel-group 2	
98	exit	
99	!	
100	interface Port-channel 1	
101	ip address 10.0.0.1 255.255.255.252	
102	mtu 1500	MTU値を指定★お客様の環境に合わせて設定お願いします。
103	mss 1360	MSS値を指定★お客様の環境に合わせて設定お願いします。
104	exit	
105	!	
106	interface Port-channel 2	
107	ip vrf forwarding VRF1	
108	ip address 192.168.0.1 255.255.255.0	
109	mtu 1500	MTU値を指定★お客様の環境に合わせて設定お願いします。
110	mss 1360	MSS値を指定★お客様の環境に合わせて設定お願いします。
111	exit	