対象装置：FITELnet F2500

	EAP-MSCHAPv2 RADIUS認証&アカウンティング 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	!	
11	ip vrf VRF1	VRF定義
12	rd 1:1	RD値を指定
13	exit	
14	!	
15	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
16	!	
17	aaa authentication ike-client AUTH1 group RADIUS1	拡張認証方法を指定(RADIUS認証)
18	aaa accounting network ACCT1 start-stop group RADIUS1	アカウンティング方法を指定
19	!	
20	aaa group server radius RADIUS1	RADIUSサーバ設定
21	server-private 192.168.0.251 key secret auth-port 1812 acct-port 1813	RADIUSサーバ指定(アドレス、共有鍵、認証用・アカウンティング用ポート指定) ※プライマリサーバ
22	server-private 192.168.0.252 key secret auth-port 1812 acct-port 1813	RADIUSサーバ指定(アドレス、共有鍵、認証用・アカウンティング用ポート指定) ※セカンダリサーバ
23	changeback-time 1	プライマリサーバへの切り戻り時間を指定(分)
24	ip vrf forwarding VRF1	VRFを指定 ※RADIUSサーバが配置されているネットワークが属すVRFを指定します。
25	nas-ip-address 192.168.0.1	RADIUSサーバに通知するNAS IPアドレス指定
26	exit	
27	!	
28	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。
29	!	
30	hostname IPsecGW	hostname指定
31	!	
32	crypto ipsec udp-encapsulation nat-t keepalive interval 60	NAT-T有効化
33	!	
34	crypto ipsec policy IPsec_POLICY	IPsecポリシー設定(Phase2 SAのパラメータを指定)
35	set security-association lifetime seconds 3600	Lifetime(秒)を指定
36	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
37	set security-association transform esp-aes 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
38	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。
39	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。
40	set ip df-bit 0	ESPパケットのDFビットを"0"に設定
41	set ip fragment post	ポストフラグメント指定
42	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。
43	exit	
44	!	
45	crypto ipsec selector SELECTOR	セレクタ設定
46	src 1 ipv4 any	送信元セレクタ(v4)を指定
47	src 2 ipv6 any	送信元セレクタ(v6)を指定
48	dst 1 ipv4 any	宛先セレクタ(v4)を指定
49	dst 2 ipv6 any	宛先セレクタ(v6)を指定
50	exit	
51	!	
52	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
53	crypto isakmp log sa detail	SYSLOGにSA確立・切断のログを出力
54	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
55	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
56	!	
57	crypto isakmp policy ISAKMP_POLICY	ISAKMPポリシー設定(Phase1 SAのパラメータを指定)
58	authentication rsa-sig	RSA認証を指定
59	encryption aes	暗号化アルゴリズムを指定(AES)
60	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
61	group 2 5 14 15	DHグループを指定(2, 5, 14, 15)
62	lifetime 86400	Lifetime(秒)を指定
63	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)
64	exit	
65	!	
66	crypto isakmp profile PROF1	ISAKMPプロファイル設定
67	local-address 10.0.0.1	ローカル側のIPsec終端アドレスを指定
68	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。
69	set isakmp-policy ISAKMP_POLICY	ISAKMPポリシーを指定
70	set ipsec-policy IPsec_POLICY	IPsecポリシーを指定
71	ca trustpoint CA1	CA証明書名を指定
72	client authentication list AUTH1	拡張認証方法を指定
73	client authentication type eap-mschapv2	認証方式にEAP MS-CHAPv2を指定
74	client authentication eap-identity request	認証時にEAP IDを要求
75	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)
76	accounting ACCT1	アカウンティング方法を指定
77	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。
78	exit	
79	!	
80	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。
81	!	
82	crypto map MAP1 ipsec-isakmp dynamic	CRYPTOマップ設定

	EAP-MSCHAPv2 RADIUS認証&アカウンティング 設定例	補足
83	match address SELECTOR	セレクタを指定
84	set isakmp-profile PROF1	ISAKMPプロファイルと紐付け
85	vrf VRF1	VRFを指定 ※暗号化対象が属すVRFを指定します。
86	exit	
87	!	
88	interface GigaEthernet 1/1	
89	ip access-group 111 in	
90	ip access-group 121 out	
91	channel-group 1	
92	exit	
93	!	
94	interface GigaEthernet 1/2	
95	channel-group 2	
96	exit	
97	!	
98	interface Port-channel 1	
99	ip address 10.0.0.1 255.255.255.252	
100	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。
101	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。
102	exit	
103	!	
104	interface Port-channel 2	
105	ip vrf forwarding VRF1	
106	ip address 192.168.0.1 255.255.255.0	
107	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。
108	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。
109	exit	