	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 121 spi ip any any	
5	!	
6	ip route 0.0.0.0 0.0.0.0 10.0.0.2	
7	ip route vrf VRF1 0.0.0.0 0.0.0.0 192.168.0.254	
8	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。
9	!	
10	ip vrf VRF1	VRF定義
11	rd 1:1	RD値を指定
12	exit	
13	!	
14	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
15	!	
16	aaa authentication ike-client AUTH1 group RADIUS1	拡張認証方法を指定(RADIUS認証)
17	aaa accounting network ACCT1 start-stop group RADIUS1	アカウンティング方法を指定
18	!	
19	aaa group server radius RADIUS1	RADIUSサーバ設定
20	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
21	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
22	changeback-time 1	プライマリサーバへの切り戻り時間を指定(分)
23	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。
24	nas-ip-address 192.168.0.1	RADIUSサーバに通知するNAS IPアドレス指定
25	exit	
26	!	
27	hostname IPsecGW	hostname指定
28	!	
29	crypto ipsec udp-encapsulation nat-t keepalive interval 60	NAT-T有効化
30	!	
31	crypto ipsec policy IPsec_POLICY	IPsecポリシー設定(Phase2 SAのパラメータを指定)
32	set security-association lifetime seconds 3600	Lifetime(秒)を指定
33	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
34	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
35	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。
36	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。
37	set ip df-bit 0	ESPパケットのDFビットを"0"に設定
38	set ip fragment post	ポストフラグメント指定
39	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。
40	exit	
41	!	
42	crypto ipsec selector SELECTOR	セレクタ設定
43	src 1 ipv4 any	送信元セレクタ(v4)を指定
44	src 2 ipv6 any	送信元セレクタ(v6)を指定
45	dst 1 ipv4 any	宛先セレクタ(v4)を指定
46	dst 2 ipv6 any	宛先セレクタ(v6)を指定
47	exit	
48	!	
49	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
50	crypto isakmp log sa detail	SYSLOGにSA確立・切断のログを出力
51	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
52	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
53	!	
54	crypto isakmp policy ISAKMP_POLICY	ISAKMPポリシー設定(Phase1 SAのパラメータを指定)
55	authentication rsa-sig	RSA認証を指定
56	encryption aes	暗号化アルゴリズムを指定(AES)
57	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
58	group 2 5 14 15	DHグループを指定(2, 5, 14, 15)
59	lifetime 86400	Lifetime(秒)を指定
60	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)
61	exit	
62	!	
63	crypto isakmp profile PROF1	ISAKMPプロファイル設定
64	local-address 10.0.0.1	ローカル側のIPsec終端アドレスを指定
65	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。
66	set isakmp-policy ISAKMP_POLICY	ISAKMPポリシーを指定
67	set ipsec-policy IPsec_POLICY	IPsecポリシーを指定
68	ca trustpoint CA1	CA証明書名を指定
69	client authentication list AUTH1	拡張認証方法を指定
70	client authentication type eap-mschapv2	認証方式にEAP MS-CHAPv2を指定
71	client authentication eap-identity request	認証時にEAP IDを要求
72	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)
73	accounting ACCT1	アカウンティング方法を指定
74	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。
75	exit	
76	!	
77	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。
78	!	
79	crypto map MAP1 ipsec-isakmp dynamic	CRYPTOマップ設定
80	match address SELECTOR	セレクタを指定
81	set isakmp-profile PROF1	ISAKMPプロファイルと紐付け
82	vrf VRF1	VRFを指定 ※暗号化対象が属すVRFを指定します。
83	exit	
84	!	

	F2500 EAP-MSCHAPv2 RADIUS認証&アカウンティング 設定例	補足
85	interface GigaEthernet 1/1	
86	ip access-group 111 in	
87	ip access-group 121 out	
88	channel-group 1	
89	exit	
90	!	
91	interface GigaEthernet 1/2	
92	channel-group 2	
93	exit	
94	!	
95	interface Port-channel 1	
96	ip address 10.0.0.1 255.255.255.252	
97	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。
98	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。
99	exit	
100	!	
101	interface Port-channel 2	
102	ip vrf forwarding VRF1	
103	ip address 192.168.0.1 255.255.255.0	
104	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。
105	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。
106	exit	