

	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 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	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
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 local-group LOCAL1	拡張認証方法を指定(Local認証)
18	aaa authorization network CP1 local-group CONFIG1	アドレス払い出し方法を指定
19	!	
20	aaa local group LOCAL1	拡張認証用ローカルデータベース設定
21	username user1 password pass1	EAPのID/Passwordを指定
22	username user2 password pass2	
23	exit	
24	!	
25	hostname IPsecGW	hostname指定
26	!	
27	crypto ipsec udp-encapsulation nat-t keepalive interval 60	NAT-T有効化
28	!	
29	crypto ipsec policy IPsec POLICY	IPsecポリシー設定(Phase2 SAのパラメータを指定)
30	set security-association lifetime seconds 3600	Lifetime(秒)を指定
31	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
32	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
33	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をお願いします。
34	set mss 1360	MSS値を指定 ★お客様の環境に合わせて設定をお願いします。
35	set ip df-bit 0	ESPパケットのDFビットを"0"に設定
36	set ip fragment post	ポストフラグメント指定
37	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。
38	exit	
39	!	
40	crypto ipsec selector SELECTOR	セレクタ設定
41	src 1 ipv4 any	送信元セレクタ(v4)を指定
42	src 2 ipv6 any	送信元セレクタ(v6)を指定
43	dst 1 ipv4 any	宛先セレクタ(v4)を指定
44	dst 2 ipv6 any	宛先セレクタ(v6)を指定
45	exit	
46	!	
47	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
48	crypto isakmp log sa detail	SYSLOGにSA確立・切断のログを出力
49	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
50	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
51	!	
52	crypto isakmp client configuration group CONFIG1	Configuration Payloadによる払い出し設定
53	pool POOL1	アドレスプール指定
54	exit	
55	!	
56	crypto isakmp policy ISAKMP POLICY	ISAKMPポリシー設定(Phase1 SAのパラメータを指定)
57	authentication rsa-sig	RSA認証を指定
58	encryption aes	暗号化アルゴリズムを指定(AES)
59	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
60	group 2 5 14 15	DHグループを指定(2, 5, 14, 15)
61	lifetime 86400	Lifetime(秒)を指定
62	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)
63	exit	
64	!	
65	crypto isakmp profile PROF1	ISAKMPプロファイル設定
66	local-address 10.0.0.1	ローカル側のIPsec終端アドレスを指定
67	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。
68	set isakmp-policy ISAKMP POLICY	ISAKMPポリシーを指定
69	set ipsec-policy IPsec POLICY	IPsecポリシーを指定
70	ca trustpoint CA1	CA証明書名を指定
71	client authentication list AUTH1	拡張認証方法を指定
72	client authentication type eap-mschapv2	認証方式にEAP-MS-CHAPv2を指定
73	client authentication eap-identity request	認証時にEAP IDを要求
74	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)
75	isakmp authorization list CP1	Configuration Payloadによる払い出し情報を指定
76	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"cr1"、または"cr1 none"を指定して下さい。
77	exit	

	F2500 EAP-MSCHAPv2 Local認証 設定例	補足
78	!	
79	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。
80	!	
81	crypto map MAP1 ipsec-isakmp dynamic	CRYPTOマップ設定
82	match address SELECTOR	セレクタを指定
83	set isakmp-profile PROF1	ISAKMPプロファイルと紐付け
84	vrf VRF1	VRFを指定 ※暗号化対象が属すVRFを指定します。
85	exit	
86	!	
87	interface GigaEthernet 1/1	
88	ip access-group 111 in	
89	ip access-group 121 out	
90	channel-group 1	
91	exit	
92	!	
93	interface GigaEthernet 1/2	
94	channel-group 2	
95	exit	
96	!	
97	interface Port-channel 1	
98	ip address 10.0.0.1 255.255.255.252	
99	mtu 1500	MTU値を指定★お客様の環境に合わせて設定をお願いします。
100	mss 1360	MSS値を指定★お客様の環境に合わせて設定をお願いします。
101	exit	
102	!	
103	interface Port-channel 2	
104	ip vrf forwarding VRF1	
105	ip address 192.168.0.1 255.255.255.0	
106	mtu 1500	MTU値を指定★お客様の環境に合わせて設定をお願いします。
107	mss 1360	MSS値を指定★お客様の環境に合わせて設定をお願いします。
108	exit	