

	F220 EAP-MSCHAPv2 RADIUS接続&アカウントング 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 0.0.0.0 192.168.0.254	
7	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。
8	!	
9	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
10	!	
11	aaa authentication ike-client AUTH1 group RADIUS1	拡張認証方法を指定(RADIUS認証)
12	aaa accounting network ACCT1 start-stop group RADIUS1	アカウントング方法を指定
13	!	
14	aaa group server radius RADIUS1	RADIUSサーバ設定
15	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・アカウントング用ポート指定) ※プライマリサーバ
16	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・アカウントング用ポート指定) ※セカンダリサーバ
17	changeback-time 1	プライマリサーバへの切り戻り時間を指定(分)
18	nas-ip-address 192.168.0.1	RADIUSサーバに通知するNAS IPアドレス指定
19	exit	
20	!	
21	hostname IPsecGW	hostname指定
22	!	
23	crypto ipsec udp-encapsulation nat-t keepalive interval 60	NAT-T有効化
24	!	
25	crypto ipsec policy IPsec POLICY	IPsecポリシー設定(Phase2 SAのパラメータを指定)
26	set security-association lifetime seconds 3600	Lifetime(秒)を指定
27	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
28	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
29	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。
30	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。
31	set ip df-bit 0	ESPパケットのDFビットを"0"に設定
32	set ip fragment post	ポストフラグメント指定
33	sa-up route	SA-UP経路設定
34	exit	※Configuration Payloadによる払い出しアドレス宛ての経路を登録します。
35	!	
36	crypto ipsec selector SELECTOR	セレクトラ設定
37	src 1 ipv4 any	送信元セレクトラ(v4)を指定
38	src 2 ipv6 any	送信元セレクトラ(v6)を指定
39	dst 1 ipv4 any	宛先セレクトラ(v4)を指定
40	dst 2 ipv6 any	宛先セレクトラ(v6)を指定
41	exit	
42	!	
43	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
44	crypto isakmp log sa detail	SYSLOGにSA確立・切断のログを出力
45	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。
46	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
47	crypto isakmp tunnel-route ip address 10.0.0.2	SA確立時にリモート側IPsec終端アドレス宛ての経路を指定したnexthopで登録
48	!	
49	crypto isakmp policy ISAKMP POLICY	ISAKMPポリシー設定(Phase1 SAのパラメータを指定)
50	authentication rsa-sig	RSA認証を指定
51	encryption aes	暗号化アルゴリズムを指定(AES)
52	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
53	group 2 5 14 15	DHグループを指定(2、5、14、15)
54	lifetime 86400	Lifetime(秒)を指定
55	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)
56	exit	
57	!	
58	crypto isakmp profile PROF1	ISAKMPプロファイル設定
59	local-address 10.0.0.1	ローカル側のIPsec終端アドレスを指定
60	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。
61	set isakmp-policy ISAKMP POLICY	ISAKMPポリシーを指定
62	set ipsec-policy IPsec POLICY	IPsecポリシーを指定
63	ca trustpoint CA1	CA証明書を指定
64	client authentication list AUTH1	拡張認証方法を指定
65	client authentication type eap-mschapv2	認証方式にEAP-MS-CHAPv2を指定
66	client authentication eap-identity request	認証時にEAP IDを要求
67	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)
68	accounting ACCT1	アカウントング方法を指定
69	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"crI"、または"crI none"を指定して下さい。
70	exit	
71	!	
72	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。
73	!	
74	crypto map MAP1 ipsec-isakmp dynamic	CRYPTOマップ設定
75	match address SELECTOR	セレクトラを指定
76	set isakmp-profile PROF1	ISAKMPプロファイルと紐付け
77	exit	
78	!	
79	interface GigaEthernet 1/1	
80	vlan-id 2	
81	bridge-group 2	
82	channel-group 2	
83	exit	
84	!	

	F220 EAP-MSCHAPv2 RADIUS認証&アカウントینگ 設定例	補足
85	interface GigEthernet 2/1	
86	vlan-id 1	
87	bridge-group 1	
88	channel-group 1	
89	ip access-group 111 in	
90	ip access-group 121 out	
91	exit	
92	!	
93	interface Port-channel 1	
94	ip address 10.0.0.1 255.255.255.252	
95	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。
96	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。
97	exit	
98	!	
99	interface Port-channel 2	
100	ip address 192.168.0.1 255.255.255.0	
101	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。
102	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。
103	exit	