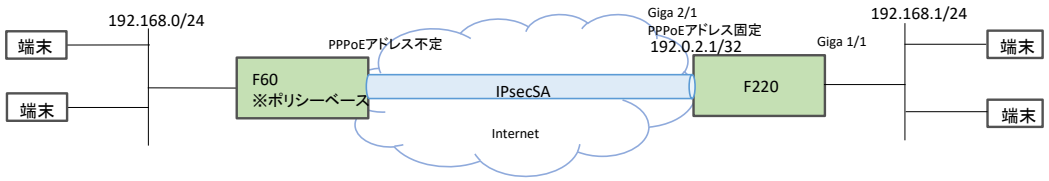
設定例

F60とIPsecでトンネリングする：F60ポリシーベース-F220ルートベース

概要

F60をポリシーベース方式として、F220とIPsecトンネリング接続するための設定例です。
・暗号化対象(IPsecセレクタ)のsrc/dstアドレス設定が双方で一致していれば、SA接続および通信可能です。
・F220のIPsecセレクタ設定ではプロトコルやポート番号は指定出来ないので、F60側のIPsecセレクタ設定もアドレスのみとしてください。
・本設定例はF60-F220間で1SAを接続する場合です。F60をポリシーベース方式としてF60-F220間で複数SAを接続する場合は、F220にてポリシールーティングを併用することにより可能です。



パラメータ設定例

ISAKMPポリシー

IKEバージョン	1
モード	Aggressiveモード
認証方式	事前共有鍵方式
暗号化方式	AES 256ビット
ハッシュ方式	SHA-1
Diffie-Hellman	Group 14
ライフタイム	86400秒

IPSECポリシー

PFS	Group 14
暗号化方式	AES 256ビット
ハッシュ方式	SHA-1
ライフタイム	28800秒
フラグメント	ポストフラグメント

コマンド設定例

F60の設定

	設定例(F60)	補足
1	ip route 0.0.0.0 0.0.0.0 pppoe 1	
2	!	
3	access-list 99 permit 192.168.0.0 0.0.0.255	
4	!	
5	vpn enable	
6	vpnlog enable	
7	!	
8	ipsec access-list 1 ipsec ip 192.168.0.0 0.0.0.255 192.168.1.0 0.0.0.255	
9	ipsec access-list 64 bypass ip any any	
10	ipsec transform-set P2-POLICY esp-aes-256 esp-sha-hmac	
11	!	
12	interface lan 1	
13	ip address 192.168.0.254 255.255.255.0	
14	exit	
15	interface pppoe 1	
16	crypto map CENTER	
17	ip nat inside source list 99 interface	
18	pppoe server FLETS-ADSL	
19	pppoe account abc345@***.***.ne.jp zzzyyyxxx	
20	pppoe type host	
21	exit	
22	!	
23	crypto isakmp policy 1	
24	authentication prekey	
25	encryption aes 256	
26	group 14	
27	hash sha	
28	idtype-pre userfqdn	
29	key ascii SECRET-VPN	
30	lifetime 86400	
31	my-identity id-kyoten	
32	negotiation-mode aggressive	
33	peer-identity address 192.0.2.1	
34	exit	
35	crypto map CENTER 1	
36	match address 1	
37	set peer address 192.0.2.1	
38	set pfs group14	
39	set security-association lifetime seconds 28800	
40	set security-association always-up	
41	set transform-set P2-POLICY	
42	exit	
43	!	
44	end	

F220の設定

	設定例(F220)	補足
1	access-list 100 permit udp any eq 500 192.0.2.1 0.0.0.0 eq 500	VPNで使用するパケットを受信許可するフィルタリングの設定
2	access-list 100 permit 50 any 192.0.2.1 0.0.0.0	VPNで使用するパケットを受信許可するフィルタリングの設定
3	access-list 111 deny ip any any	学習フィルタリングの設定
4	access-list 121 spi ip any any	学習フィルタリングの設定
5	!	
6	ip route 0.0.0.0 0.0.0.0 tunnel 1	
7	ip route 192.168.0.0 255.255.255.0 tunnel 2	F60のLANネットワークへのTunnel(IPsec)経路を登録
8	ip nat list 1 192.168.1.0 0.0.0.255	
9	!	
10	logging level informational	isakmpログを記録するためにログレベルを設定
11	!	
12	crypto ipsec policy P2-POLICY	IPsecポリシー設定(共有設定)
13	set pfs group14	
14	set security-association lifetime seconds 28800	
15	set security-association transform-keysize aes 256 256 256	
16	set security-association transform esp-aes esp-sha-hmac	
17	set mtu 1454	
18	set ip df-bit 0	
19	set ip fragment post	
20	exit	
21	!	
22	crypto ipsec selector SELECTOR0001	セレクタ設定(対向拠点毎に設定)
23	src 1 ipv4 192.168.1.0 255.255.255.0	送信元セレクタをF220のLANネットワークを対象に設定
24	dst 1 ipv4 192.168.0.0 255.255.255.0	宛先セレクタをF60のLANネットワークを対象に設定
25	exit	
26	!	
27	crypto isakmp keepalive	
28	crypto isakmp log sa	
29	crypto isakmp log session	
30	crypto isakmp log negotiation-fail	
31	!	
32	crypto isakmp policy P1-POLICY	ISAKMPポリシー設定(共有設定)
33	authentication pre-share	
34	encryption aes	
35	encryption-keysize aes 256 256 256	
36	group 14	
37	lifetime 86400	
38	hash sha	
39	initiate-mode aggressive	
40	exit	
41	!	
42	crypto isakmp profile PROF0001	ISAKMPプロファイル設定(対向拠点毎に設定)
43	match identity user id-kyoten	
44	local-address 192.0.2.1	
45	set isakmp-policy P1-POLICY	
46	set ipsec-policy P2-POLICY	
47	ike-version 1	
48	local-key SECRET-VPN	
49	exit	
50	!	
51	crypto map KYOTEN0001 ipsec-isakmp	CRYPTO MAP設定(対向拠点毎に設定)
52	match address SELECTOR0001	
53	set isakmp-profile PROF0001	
54	exit	
55	!	
56	interface GigaEthernet 1/1	
57	vlan-id 1	
58	bridge-group 1	
59	channel-group 1	
60	exit	
61	!	
62	interface GigaEthernet 2/1	
63	vlan-id 2	
64	bridge-group 2	
65	pppoe enable	
66	exit	
67	!	
68	interface Port-channel 1	
69	ip address 192.168.1.254 255.255.255.0	
70	mss 1300	
71	exit	
72	!	
73	interface Tunnel 1	
74	description FLETS	
75	ip address 192.0.2.1 255.255.255.255	
76	ip access-group 100 in	
77	ip access-group 111 in	
78	ip access-group 121 out	
79	ip nat inside source list 1 interface	
80	tunnel mode pppoe profile PPPOE_PROF0001	
81	pppoe interface gigaethernet 2/1	
82	exit	
83	!	
84	interface Tunnel 2	Tunnel(IPsec)インタフェース設定(対向拠点毎に設定)
85	tunnel mode ipsec map KYOTEN0001	
86	exit	
87	!	
88	pppoe profile PPPOE_PROF	
89	account abc012@***.***.ne.jp xxxyyyzzz	
90	exit	
91	!	
92	end	