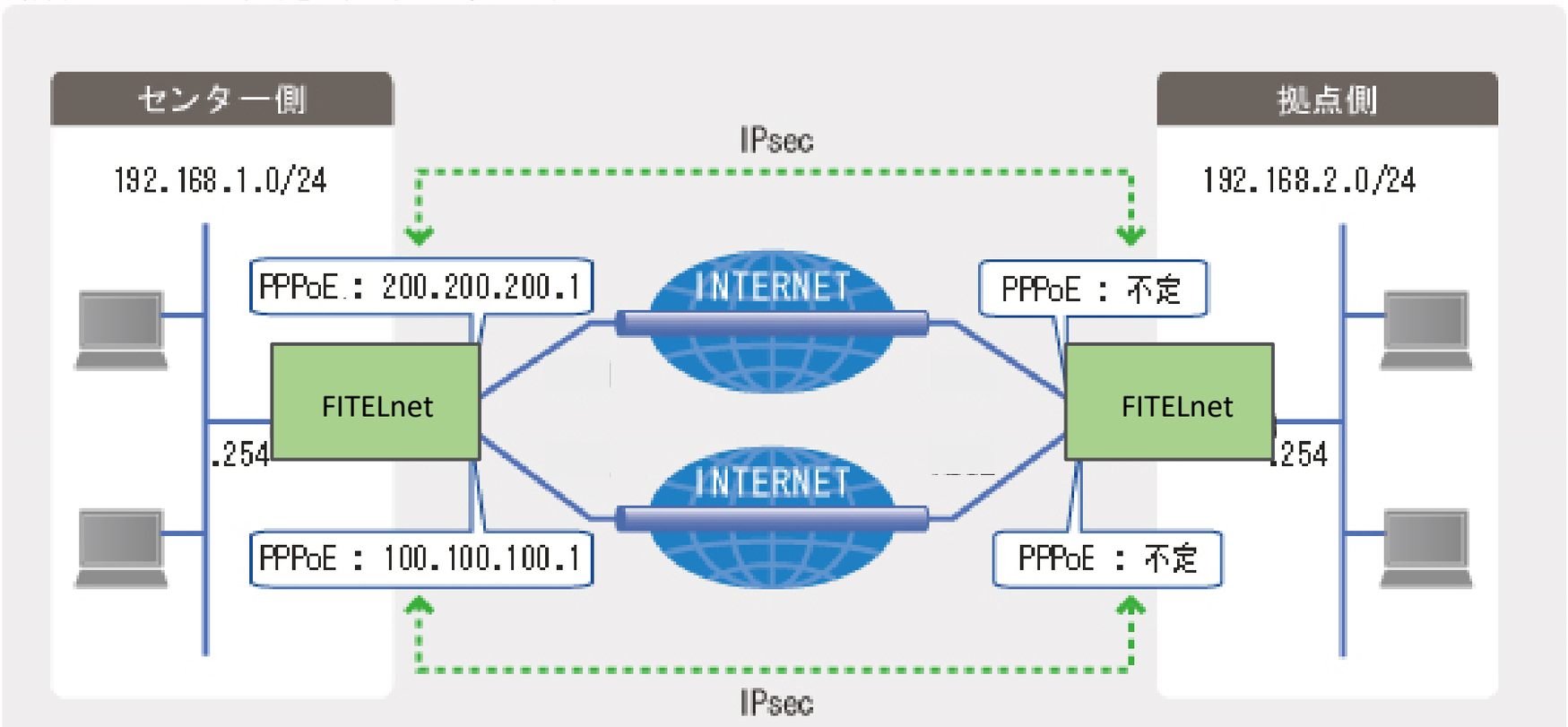
設定例

IPsec冗長：センタ、拠点各1台でIPsec/PPPoE冗長～イベントアクションでバックアップ側経路制御

概要

イベントアクション機能を使って、通常時はメイン側PPPoE回線のIPsecで通信を行い、メイン回線に障害が発生したときにはバックアップ側PPPoE回線のIPsecで通信を行う構成です。
・拠点側はメイン回線のIPsecトンネル経由で、センタ側のLANインタフェースをsurvey監視します。
・拠点側のsurvey監視がダウンしたら、イベントアクション機能を利用して、バックアップ回線のIPsecトンネルに向けた経路を追加して、経路の切り替えを行います。その後、survey監視がアップしたら、バックアップ回線のIPsecトンネルに向けた経路を削除することで、経路を切り戻します。
・センタ側は Phase 2 SAの有無に応じて登録／削除されるSA-Up経路を利用して経路の切り替え、切り戻しを行います。
（FITELnetが1台の構成で、同一のSA-Upルートを複数のSAで登録する動作は不可となる仕様のため、メイン回線側ではSA-Up経路を、バックアップ回線側ではスタティック経路を、それぞれ登録します。）



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-256
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-256
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

センタ側FITELnetの設定

	設定例	補足
1	access-list 100 permit udp any eq 500 200.200.200.1 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 200.200.200.1 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 101 permit udp any eq 500 100.100.100.1 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
4	access-list 101 permit 50 any 100.100.100.1 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
5	access-list 111 deny ip any any	学習フィルタリングの設定
6	access-list 121 spi ip any any	学習フィルタリングの設定
7		
8	ip route 192.168.2.0 255.255.255.0 tunnel 2 50	SA-Up経路を優先するためディスタンス値を大きくします
9	!	
10	crypto ipsec policy P2_POLICY_BACKUP	
11	set pfs group14	
12	set security-association lifetime seconds 28800	
13	set security-association transform-keysize aes 256 256 256	
14	set security-association transform esp-sha256-hmac	
15	set mtu 1454	
16	set ip df-bit 0	
17	set ip fragment post	
18	exit	
19	!	
20	crypto ipsec policy P2_POLICY_MAIN	
21	set pfs group14	
22	set security-association lifetime seconds 28800	
23	set security-association transform-keysize aes 256 256 256	
24	set security-association transform esp-sha256-hmac	
25	set mtu 1454	
26	set ip df-bit 0	
27	set ip fragment post	
28	sa-up route distance 1	生成されたSAのセレクタの宛先情報を経路情報として登録する設定です（SA-Up経路登録）

	設定例	補足
29	exit	
30	!	
31	crypto ipsec selector SELECTOR_BACKUP	
32	src 1 ipv4 any	
33	dst 1 ipv4 any	
34	exit	
35	!	
36	crypto ipsec selector SELECTOR_MAIN_0001	SA-Up経路を使用するため拠点/センタのネットワークを指定します
37	src 1 ipv4 192.168.1.0 255.255.255.0	
38	dst 1 ipv4 192.168.2.0 255.255.255.0	
39	exit	
40	!	
41	crypto isakmp log sa	
42	crypto isakmp log session	
43	crypto isakmp log negotiation-fail	
44	!	
45	crypto isakmp policy P1-POLICY	
46	authentication pre-share	
47	encryption aes	
48	encryption-keysize aes 256 256 256	
49	group 14	
50	lifetime 86400	
51	hash sha-256	
52	initiate-mode aggressive	
53	exit	
54	!	
55	crypto isakmp profile P1_PROFILE_1	
56	match identity user Kyoten_1@furukawa.co.jp	
57	local-address 200.200.200.1	
58	keepalive interval 10	DPD KeepAlive指定（インターバル10秒）
59	set isakmp-policy P1-POLICY	
60	set ipsec-policy P2_POLICY_MAIN	
61	ike-version 1	
62	local-key secret	
63	tunnel-route ip interface tunnel 101	
64	exit	
65	!	
66	crypto isakmp profile P1_PROFILE_2	
67	match identity user Kyoten_2@furukawa.co.jp	
68	local-address 100.100.100.1	
69	keepalive interval 10	DPD KeepAlive指定（インターバル10秒）
70	set isakmp-policy P1-POLICY	
71	set ipsec-policy P2_POLICY_BACKUP	
72	ike-version 1	
73	local-key secret	
74	tunnel-route ip interface tunnel 102	
75	exit	
76	!	
77	crypto map CryptoMap_1 ipsec-isakmp	
78	match address SELECTOR_MAIN_0001	
79	set isakmp-profile P1_PROFILE_1	
80	exit	
81	!	
82	crypto map CryptoMap_2 ipsec-isakmp	
83	match address SELECTOR_BACKUP	
84	set isakmp-profile P1_PROFILE_2	
85	exit	
86	!	
87	interface GigaEthernet 1/1	
88	vlan-id 11	
89	bridge-group 11	
90	channel-group 11	
91	exit	
92	!	
93	interface GigaEthernet 2/1	
94	vlan-id 21	
95	bridge-group 21	
96	pppoe enable	
97	exit	
98	!	
99	interface GigaEthernet 3/1	
100	vlan-id 31	
101	bridge-group 31	
102	pppoe enable	
103	exit	
104	!	
105	interface Port-channel 11	
106	ip address 192.168.1.254 255.255.255.0	
107	exit	
108	!	
109	interface Tunnel 1	
110	tunnel mode ipsec map CryptoMap_1	
111	exit	
112	!	
113	interface Tunnel 2	
114	tunnel mode ipsec map CryptoMap_2	
115	exit	
116	!	
117	interface Tunnel 101	
118	ip address 200.200.200.1 255.255.255.0	
119	ip access-group 100 in	
120	ip access-group 111 in	
121	ip access-group 121 out	
122	tunnel mode pppoe profile PPPoE_MAIN	
123	pppoe interface gigaethernet 2/1	
124	exit	
125	!	

	設定例	補足
126	interface Tunnel 102	
127	ip address 100.100.100.1 255.255.255.0	
128	ip access-group 101 in	
129	ip access-group 111 in	
130	ip access-group 121 out	
131	tunnel mode pppoe profile PPPoE_BACKUP	
132	pppoe interface gigaethernet 3/1	
133	exit	
134	!	
135	pppoe profile PPPoE_BACKUP	
136	account user2@xxxx.ne.jp secret2	
137	ncp ipcp	
138	exit	
139	!	
140	pppoe profile PPPoE_MAIN	
141	account user1@xxxx.ne.jp secret1	
142	ncp ipcp	
143	exit	
144	!	
145	!	
146	end	

拠点側FITELnetの設定

	設定例	補足
1	access-list 100 permit udp 200.200.200.1 0.0.0.0 eq 500 any 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 50 200.200.200.1 0.0.0.0 any	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 101 permit udp 100.100.100.1 0.0.0.0 eq 500 any 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
4	access-list 101 permit 50 100.100.100.1 0.0.0.0 any	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
5	access-list 111 deny ip any any	学習フィルタリングの設定
6	access-list 121 spi ip any any	学習フィルタリングの設定
7	!	
8	ip route 100.100.100.1 255.255.255.255 tunnel 102	バックアップのIPsecピア接続先経路
9	ip route 192.168.1.0 255.255.255.0 tunnel 1 50	メインのIPsec暗号化通信用経路：event_trackを優先するためディスタンス値を大きくします
10	ip route 192.168.1.0 255.255.255.0 tunnel 2 event-track event_track 10	バックアップのIPsec暗号化通信用経路：event_track up時に有効になります
11	ip route 200.200.200.1 255.255.255.255 tunnel 101	メインのIPsecピア接続先経路
12	!	
13	event-track event_track	event_track名を設定します
14	!	
15	survey 192.168.1.254 name survey survey-map survey_map source port-channel 11 nexthop tunnel 1	survey（ICMP）によりメイン経路を監視します
16	!	
17	survey-map survey_map	survey（ICMP）の条件を設定します
18	ttl 255	
19	hop-limit 255	
20	retry 3	リトライ3回
21	frequency every 10000	定期監視間隔10秒
22	exit	
23	!	
24	event-action 1	イベントアクション設定 1
25	event survey survey down	イベント：servey down
26	action 1.1 event-track event_track up	アクション：event_track up
27	exit	
28	!	
29	event-action 2	イベントアクション設定 2
30	event survey survey up	イベント：servey up
31	action 1.1 event-track event_track down	アクション：event_track down
32	exit	
33	!	
34	crypto ipsec policy P2_POLICY_BACKUP	
35	set pfs group14	
36	set security-association lifetime seconds 28800	
37	set security-association transform-keysize aes 256 256 256	
38	set security-association transform esp-sha256-hmac	
39	set mtu 1454	
40	set mss 1300	IPsecトンネルの先のホストから送信されたDFビットつきのTCPパケットがPPPoE回線で破棄されてしまうようなケースを考慮して、インナーのMTU長以下になるようにMSSの書き換え設定を行います。 センター経由でインターネット上のサーバと通信を行うような場合に、本設定を推奨します。
41	set ip df-bit 0	
42	set ip fragment post	
43	exit	
44	!	
45	crypto ipsec policy P2_POLICY_MAIN	
46	set pfs group14	
47	set security-association lifetime seconds 28800	
48	set security-association transform-keysize aes 256 256 256	
49	set security-association transform esp-sha256-hmac	
50	set mtu 1454	
51	set mss 1300	
52	set ip df-bit 0	
53	set ip fragment post	
54	exit	
55	!	
56	crypto ipsec selector SELECTOR_MAIN	センタ側でsa-up経路を使用するため拠点/センタのネットワークを指定します
57	src 1 ipv4 192.168.2.0 255.255.255.0	
58	dst 1 ipv4 192.168.1.0 255.255.255.0	
59	exit	
60	!	
61	crypto ipsec selector SELECTOR_BACKUP	
62	src 1 ipv4 any	
63	dst 1 ipv4 any	
64	exit	
65	!	

	設定例	補足
66	crypto isakmp log sa	
67	crypto isakmp log session	
68	crypto isakmp log negotiation-fail	
69	!	
70	crypto isakmp policy P1-POLICY	
71	authentication pre-share	
72	encryption aes	
73	encryption-keysize aes 256 256 256	
74	group 14	
75	lifetime 86400	
76	hash sha-256	
77	initiate-mode aggressive	
78	exit	
79	!	
80	crypto isakmp profile P1_PROFILE_1	
81	keepalive interval 10	DPD KeepAlive指定（インターバル10秒）
82	self-identity user-fqdn Kyoten_1@furukawa.co.jp	
83	set isakmp-policy P1-POLICY	
84	set ipsec-policy P2_POLICY_MAIN	
85	set peer 200.200.200.1	
86	ike-version 1	
87	local-key secret	
88	exit	
89	!	
90	crypto isakmp profile P1_PROFILE_2	
91	keepalive interval 10	DPD KeepAlive指定（インターバル10秒）
92	self-identity user-fqdn Kyoten_2@furukawa.co.jp	
93	set isakmp-policy P1-POLICY	
94	set ipsec-policy P2_POLICY_BACKUP	
95	set peer 100.100.100.1	
96	ike-version 1	
97	local-key secret	
98	exit	
99	!	
100	crypto map CryptoMap_1 ipsec-isakmp	
101	match address SELECTOR_MAIN	
102	set isakmp-profile P1_PROFILE_1	
103	exit	
104	!	
105	crypto map CryptoMap_2 ipsec-isakmp	
106	match address SELECTOR_BACKUP	
107	set isakmp-profile P1_PROFILE_2	
108	exit	
109	!	
110	interface GigaEthernet 1/1	
111	vlan-id 11	
112	bridge-group 11	
113	channel-group 11	
114	exit	
115	!	
116	interface GigaEthernet 2/1	
117	vlan-id 21	
118	bridge-group 21	
119	pppoe enable	
120	exit	
121	!	
122	interface GigaEthernet 3/1	
123	vlan-id 31	
124	bridge-group 31	
125	pppoe enable	
126	exit	
127	!	
128	interface Port-channel 11	
129	ip address 192.168.2.254 255.255.255.0	
130	exit	
131	!	
132	interface Tunnel 1	
133	tunnel mode ipsec map CryptoMap_1	
134	exit	
135	!	
136	interface Tunnel 2	
137	tunnel mode ipsec map CryptoMap_2	
138	exit	
139	!	
140	interface Tunnel 101	
141	tunnel mode pppoe profile PPPoE_MAIN	
142	ip access-group 100 in	
143	ip access-group 111 in	
144	ip access-group 121 out	
145	pppoe interface gigaethernet 2/1	
146	exit	
147	!	
148	interface Tunnel 102	
149	tunnel mode pppoe profile PPPoE_BACKUP	
150	ip access-group 101 in	
151	ip access-group 111 in	
152	ip access-group 121 out	
153	pppoe interface gigaethernet 3/1	
154	exit	
155	!	
156	pppoe profile PPPoE_BACKUP	
157	account user2@yyyy.ne.jp secret2	
158	ncp ipcp	
159	exit	
160	!	

	設定例	補足
161	pppoe profile PPPoE_MAIN	
162	account user1@yyyy.ne.jp secret1	
163	ncp ipcp	
164	exit	
165	!	
166	!	
167	end	