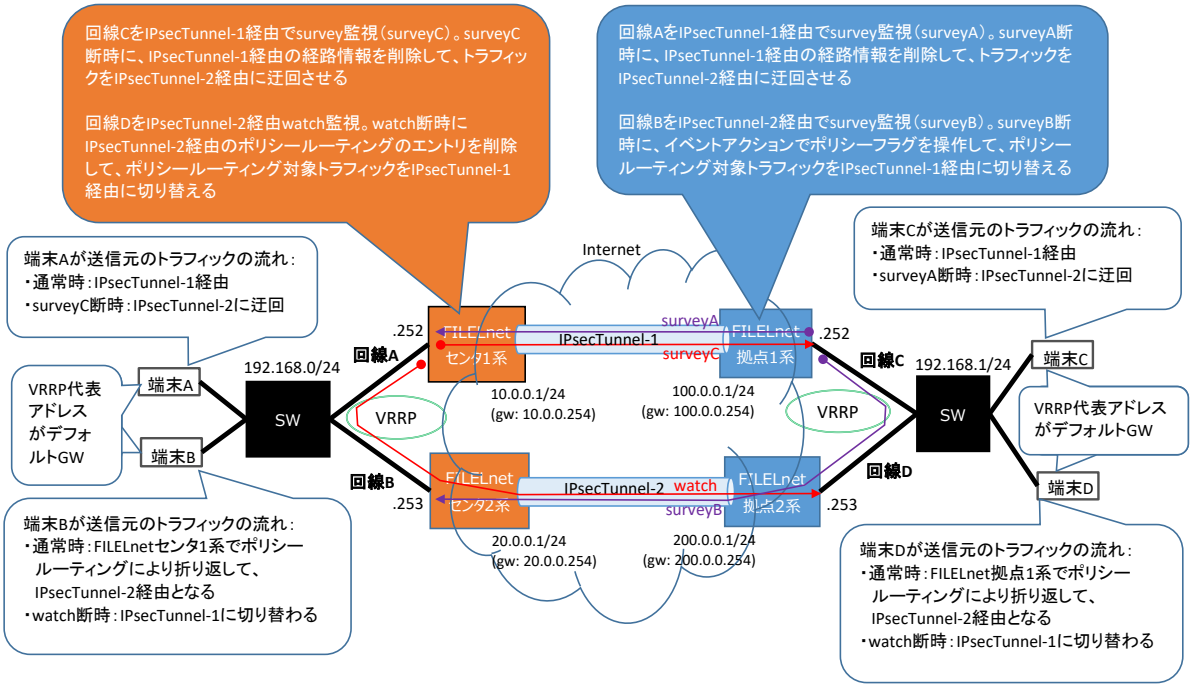
設定例

ポリシールーティング・ポリシーフラグを使って負荷分散

概要

装置および回線冗長している構成で、ポリシールーティングとポリシーフラグを利用して負荷分散を行うための設定例です。
どちらかの装置もしくは回線断となった場合には、もう片方の装置および回線にトラフィックを集約します。



本設定例は、インターネット向けの通信には対応しておりません。インターネット向けの通信を合わせて行う場合には、
デフォルトルートの設定と、必要に応じてWAN側インタフェースに学習フィルタやNATの設定を行ってください。

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1系FITELnetの設定

	設定例(センタ)	補足
1	access-list 100 permit ip 192.168.0.2 0.0.0.0 any	送信元アドレスが端末B、送信先が全てのフィルタ設定
2	access-list 110 permit udp any eq 500 10.0.0.1 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
3	access-list 110 permit 50 any 10.0.0.1 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
4	access-list 111 deny ip any any	access-list 110以外を受信拒否する設定(インターネットからのアタック防止)
5	!	
6	ip route 100.0.0.1 255.255.255.255 10.0.0.254	VPNのpeer宛経路設定
7	ip route 192.168.1.0 255.255.255.0 192.168.0.253 50	バックアップ経路設定、メイン経路を優先するためディスタンス値を大きくする
8	ip route 192.168.1.0 255.255.255.0 tunnel 1 survey name main_point 10	メイン経路設定、メイン経路の監視を行い正常な場合に適用します
9	ip route 192.168.1.253 255.255.255.255 192.168.0.253	バックアップ監視用の経路設定
10	ip route 192.168.1.253 255.255.255.255 null 0 200	バックアップ監視用経路(192.168.1.253/32)が無効となった場合に、監視パケット(watch設定)を破棄するための設定
11	ip vrrp enable	VRRP 機能を有効
12	!	
13	survey 192.168.1.252 name main_point survey-map survey_map source port-channel 1 nexthop tunnel 1	メイン経路監視
14	!	
15	survey-map survey_map	survey条件設定
16	ttl 255	TTL指定
17	retry 3	リトライ回数指定
18	frequency every 10000	定期送信間隔指定(msec)
19	exit	
20	!	
21	crypto ipsec policy P2_POLICY	
22	set pfs group14	

	設定例(センタ)	補足
23	set security-association lifetime seconds 28800	
24	set security-association transform-keysize aes 256 256 256	
25	set security-association transform esp-sha256-hmac	
26	set ip df-bit 0	
27	set ip fragment post	
28	exit	
29	!	
30	crypto ipsec selector SELECTOR	
31	src 1 ipv4 any	
32	dst 1 ipv4 any	
33	exit	
34	!	
35	crypto isakmp log sa	
36	crypto isakmp log session	
37	crypto isakmp log negotiation-fail	
38	!	
39	crypto isakmp policy P1-POLICY	
40	authentication pre-share	
41	encryption aes	
42	encryption-keysize aes 256 256 256	
43	group 14	
44	lifetime 86400	
45	hash sha-256	
46	initiate-mode aggressive	
47	exit	
48	!	
49	crypto isakmp profile P1_PROFILE_0001	
50	match identity user Kyoten_A@furukawa.co.jp	
51	local-address 10.0.0.1	
52	keepalive interval 10	DPD KeepAlive指定(インターバル10秒)
53	set isakmp-policy P1-POLICY	
54	set ipsec-policy P2_POLICY	
55	ike-version 1	
56	local-key secret	
57	exit	
58	!	
59	crypto map CryptoMap_0001 ipsec-isakmp	
60	match address SELECTOR	
61	set isakmp-profile P1_PROFILE_0001	
62	exit	
63	!	
64	interface GigaEthernet 1/1	
65	vlan-id 1	
66	bridge-group 1	
67	channel-group 1	
68	policy-route input PBR	ポリシールート設定(受信パケット)
69	exit	
70	!	
71	interface GigaEthernet 2/1	
72	vlan-id 2	
73	bridge-group 2	
74	channel-group 2	
75	ip access-group 110 in	
76	ip access-group 111 in	
77	exit	
78	!	
79	interface Port-channel 1	
80	ip address 192.168.0.252 255.255.255.0	
81	vrrp 1 address 192.168.0.254	ルータグループの仮想IPv4アドレスの設定
82	vrrp 1 priority 100	VRRPルータの優先度の設定(大きい数字ほど優先度は高くなります)
83	vrrp 1 adver-interval 10	ADVERTISEMENTパケットの送信間隔を設定します
84	vrrp 1 preempt	vrrp priorityコマンドで設定した優先度で判断し、常に優先度の高いルータがMasterルータとします。
85	exit	
86	!	
87	interface Port-channel 2	
88	ip address 10.0.0.1 255.255.255.0	
89	exit	
90	!	
91	interface Tunnel 1	
92	tunnel mode ipsec map CryptoMap_0001	
93	exit	
94	!	
95	class-map Backup	クラスマップ設定
96	match ip access-group 100	フィルタを指定します
97	exit	
98	!	
99	policy-route-map PBR	ポリシールート条件設定
100	!	
101	class Backup	クラスマップ名を指定します
102	count	マッチしたパケット数をカウントします
103	action nexthop 192.168.0.253	送信先を指定します
104	watch 192.168.1.253 source port-channel 1 survey-map survey_map	バックアップ経路の監視を行い正常な場合に適用します
105	exit	
106	!	
107	exit	
108	!	
109	end	

センタ2系FITELnetの設定

	設定例(センタ)	補足
1	access-list 110 permit udp any eq 500 20.0.0.1 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 110 permit 50 any 20.0.0.1 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	access-list 110以外を受信拒否する設定(インターネットからのアタック防止)
4	!	

	設定例(センタ)	補足
5	ip route 200.0.0.1 255.255.255.255 20.0.0.254	VPNのpeer宛経路設定
6	ip route 192.168.1.0 255.255.255.0 tunnel 1	
7	ip vrrp enable	
8	!	
9	crypto ipsec policy P2_POLICY	
10	set pfs group14	
11	set security-association lifetime seconds 28800	
12	set security-association transform-keysize aes 256 256 256	
13	set security-association transform esp-sha256-hmac	
14	set ip df-bit 0	
15	set ip fragment post	
16	exit	
17	!	
18	crypto ipsec selector SELECTOR	
19	src 1 ipv4 any	
20	dst 1 ipv4 any	
21	exit	
22	!	
23	crypto isakmp log sa	
24	crypto isakmp log session	
25	crypto isakmp log negotiation-fail	
26	!	
27	crypto isakmp policy P1-POLICY	
28	authentication pre-share	
29	encryption aes	
30	encryption-keysize aes 256 256 256	
31	group 14	
32	lifetime 86400	
33	hash sha-256	
34	initiate-mode aggressive	
35	exit	
36	!	
37	crypto isakmp profile P1_PROFILE_0001	
38	match identity user Kyoten_B@furukawa.co.jp	
39	local-address 20.0.0.1	
40	keepalive interval 10	DPD KeepAlive指定(インターバル10秒)
41	set isakmp-policy P1-POLICY	
42	set ipsec-policy P2_POLICY	
43	ike-version 1	
44	local-key secret	
45	exit	
46	!	
47	crypto map CryptoMap_0001 ipsec-isakmp	
48	match address SELECTOR	
49	set isakmp-profile P1_PROFILE_0001	
50	exit	
51	!	
52	interface GigaEthernet 1/1	
53	vlan-id 1	
54	bridge-group 1	
55	channel-group 1	
56	exit	
57	!	
58	interface GigaEthernet 2/1	
59	vlan-id 2	
60	bridge-group 2	
61	channel-group 2	
62	ip access-group 110 in	
63	ip access-group 111 in	
64	exit	
65	!	
66	interface Port-channel 1	
67	ip address 192.168.0.253 255.255.255.0	
68	vrrp 1 address 192.168.0.254	ルータグループの仮想IPv4アドレスの設定
69	vrrp 1 priority 50	VRRPルータの優先度の設定(大きい数字ほど優先度は高くなります)
70	vrrp 1 adver-interval 10	ADVERTISEMENTパケットの送信間隔を設定します
71	vrrp 1 preempt	vrrp priorityコマンドで設定した優先度で判断し、常に優先度の高いルータがMasterルータとします。
72	exit	
73	!	
74	interface Port-channel 2	
75	ip address 20.0.0.1 255.255.255.0	
76	exit	
77	!	
78	interface Tunnel 1	
79	tunnel mode ipsec map CryptoMap_0001	
80	exit	
81	!	
82	end	

拠点1系FITELnetの設定

	設定例(拠点)	補足
1	access-list 100 permit ip any 192.168.0.2 0.0.0.0	送信元が全て、送信先が端末Bアドレスのフィルタ設定
2	access-list 110 permit udp 10.0.0.1 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
3	access-list 110 permit 50 10.0.0.1 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
4	access-list 111 deny ip any any	access-list 110以外を受信拒否する設定(インターネットからのアタック防止)
5	!	
6	ip route 10.0.0.1 255.255.255.255 100.0.0.254	VPNのpeer宛経路設定
7	ip route 192.168.0.0 255.255.255.0 192.168.1.253 50	バックアップ経路設定、メイン経路を優先するためディスタンス値を大きくする
8	ip route 192.168.0.0 255.255.255.0 tunnel 1 survey name main_point 10	メイン経路設定、メイン経路の監視を行い正常な場合に適用します
9	ip vrrp enable	
10	!	
11	survey 192.168.0.252 name main_point survey-map survey_map source port-channel 1 nexthop tunnel 1	メイン経路監視
12	survey 192.168.0.253 name backup_point survey-map survey_map source port-channel 1 nexthop 192.168.1.253	バックアップ経路監視
13	!	
14	survey-map survey_map	survey条件設定
15	ttl 255	TTL指定
16	retry 3	リトライ回数指定
17	frequency every 10000	定期送信間隔指定(msec)
18	exit	
19	!	
20	event-action 1	イベントアクション設定
21	event survey backup_point down	イベント指定、バックアップ監視がdownした場合に適用
22	action 1.1 cli exec command policy-flag 1 unset	アクション指定、ポリシーフラグをunsetに遷移する
23	action 1.2 syslog message EVENT-ACTION NO1 IS FINISH.	アクション指定、syslogを記録する(送信メッセージを指定する)
24	exit	
25	!	
26	event-action 2	イベントアクション設定
27	event survey backup_point up	イベント指定、バックアップ監視がupした場合に適用
28	action 1.1 cli exec command policy-flag 1 set	アクション指定、ポリシーフラグをsetに遷移する
29	action 1.2 syslog message EVENT-ACTION NO2 IS FINISH.	アクション指定、syslogを記録する(送信メッセージを指定する)
30	exit	
31	!	
32	crypto ipsec policy P2_POLICY	
33	set pfs group14	
34	set security-association lifetime seconds 28800	
35	set security-association transform-keysize aes 256 256 256	
36	set security-association transform esp-sha256-hmac	
37	set ip df-bit 0	
38	set ip fragment post	
39	exit	
40	!	
41	crypto ipsec selector SELECTOR	
42	src 1 ipv4 any	
43	dst 1 ipv4 any	
44	exit	
45	!	
46	crypto isakmp log sa	
47	crypto isakmp log session	
48	crypto isakmp log negotiation-fail	
49	!	
50	crypto isakmp policy P1-POLICY	
51	authentication pre-share	
52	encryption aes	
53	encryption-keysize aes 256 256 256	
54	group 14	
55	lifetime 86400	
56	hash sha-256	
57	initiate-mode aggressive	
58	exit	
59	!	
60	crypto isakmp profile P1_PROFILE_1	
61	local-address 100.0.0.1	
62	keepalive interval 10	DPD KeepAlive指定(インターバル10秒)
63	self-identity user-fqdn Kyoten_A@furukawa.co.jp	
64	set isakmp-policy P1-POLICY	
65	set ipsec-policy P2_POLICY	
66	set peer 10.0.0.1	
67	ike-version 1	
68	local-key secret	
69	exit	
70	!	
71	crypto map CryptoMap_1 ipsec-isakmp	
72	match address SELECTOR	
73	set isakmp-profile P1_PROFILE_1	
74	exit	
75	!	
76	interface GigaEthernet 1/1	
77	vlan-id 1	
78	bridge-group 1	
79	channel-group 1	
80	policy-route input PBR	ポリシールート設定(受信パケット)
81	exit	
82	!	
83	interface GigaEthernet 2/1	
84	vlan-id 2	
85	bridge-group 2	
86	channel-group 2	
87	ip access-group 110 in	
88	ip access-group 111 in	
89	exit	
90	!	
91	interface Port-channel 1	
92	ip address 192.168.1.252 255.255.255.0	

	設定例(拠点)	補足
93	vrrp 1 address 192.168.1.254	ルータグループの仮想IPv4アドレスの設定
94	vrrp 1 priority 100	VRRPルータの優先度の設定(大きい数字ほど優先度は高くなります)
95	vrrp 1 adver-interval 10	ADVERTISEMENTパケットの送信間隔を設定します
96	vrrp 1 preempt	vrrp priorityコマンドで設定した優先度で判断し、常に優先度の高いルータがMasterルータとします。
97	exit	
98	!	
99	interface Port-channel 2	
100	ip address 100.0.0.1 255.255.255.0	
101	exit	
102	!	
103	interface Tunnel 1	
104	tunnel mode ipsec map CryptoMap_1	
105	exit	
106	!	
107	class-map Backup	クラスマップ設定
108	match ip access-group 100	フィルタを指定します
109	match policy-flag 1 set	ポリシーフラグがsetの場合に適用します
110	exit	
111	!	
112	policy-route-map PBR	ポリシールート条件設定
113	!	
114	class Backup	クラスマップ名を指定します
115	count	マッチしたパケット数をカウントします
116	action nexthop 192.168.1.253	送信先を指定します
117	exit	
118	!	
119	exit	
120	!	
121	end	

拠点2系FITELnetの設定

	設定例(拠点)	補足
1	access-list 110 permit udp 20.0.0.1 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 110 permit 50 20.0.0.1 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 111 deny ip any any	access-list 110以外を受信拒否する設定(インターネットからのアタック防止)
4	!	
5	ip route 20.0.0.1 255.255.255.255 200.0.0.254	VPNのpeer宛経路設定
6	ip route 192.168.0.0 255.255.255.0 tunnel 1	
7	ip vrrp enable	
8	!	
9	crypto ipsec policy P2_POLICY	
10	set pfs group14	
11	set security-association lifetime seconds 28800	
12	set security-association transform-keysize aes 256 256 256	
13	set security-association transform esp-sha256-hmac	
14	set ip df-bit 0	
15	set ip fragment post	
16	exit	
17	!	
18	crypto ipsec selector SELECTOR	
19	src 1 ipv4 any	
20	dst 1 ipv4 any	
21	exit	
22	!	
23	crypto isakmp log sa	
24	crypto isakmp log session	
25	crypto isakmp log negotiation-fail	
26	!	
27	crypto isakmp policy P1-POLICY	
28	authentication pre-share	
29	encryption aes	
30	encryption-keysize aes 256 256 256	
31	group 14	
32	lifetime 86400	
33	hash sha-256	
34	initiate-mode aggressive	
35	exit	
36	!	
37	crypto isakmp profile P1_PROFILE_1	
38	local-address 200.0.0.1	
39	keepalive interval 10	DPD KeepAlive指定(インターバル10秒)
40	self-identity user-fqdn Kyoten_B@furukawa.co.jp	
41	set isakmp-policy P1-POLICY	
42	set ipsec-policy P2_POLICY	
43	set peer 20.0.0.1	
44	ike-version 1	
45	local-key secret	
46	exit	
47	!	
48	crypto map CryptoMap_1 ipsec-isakmp	
49	match address SELECTOR	
50	set isakmp-profile P1_PROFILE_1	
51	exit	
52	!	
53	interface GigaEthernet 1/1	
54	vlan-id 1	
55	bridge-group 1	
56	channel-group 1	
57	exit	
58	!	
59	interface GigaEthernet 2/1	
60	vlan-id 2	
61	bridge-group 2	
62	channel-group 2	
63	ip access-group 110 in	

	設定例（拠点）	補足
64	ip access-group 111 in	
65	exit	
66	!	
67	interface Port-channel 1	
68	ip address 192.168.1.253 255.255.255.0	
69	vrrp 1 address 192.168.1.254	ルータグループの仮想IPv4アドレスの設定
70	vrrp 1 priority 50	VRRPルータの優先度の設定（大きい数字ほど優先度は高くなります）
71	vrrp 1 adver-interval 10	ADVERTISEMENTパケットの送信間隔を設定します
72	vrrp 1 preempt	vrrp priorityコマンドで設定した優先度で判断し、常に優先度の高いルータがMasterルータとします。
73	exit	
74	!	
75	interface Port-channel 2	
76	ip address 200.0.0.1 255.255.255.0	
77	exit	
78	!	
79	interface Tunnel 1	
80	tunnel mode ipsec map CryptoMap_1	
81	exit	
82	!	
83	!	
84	end	