設定例

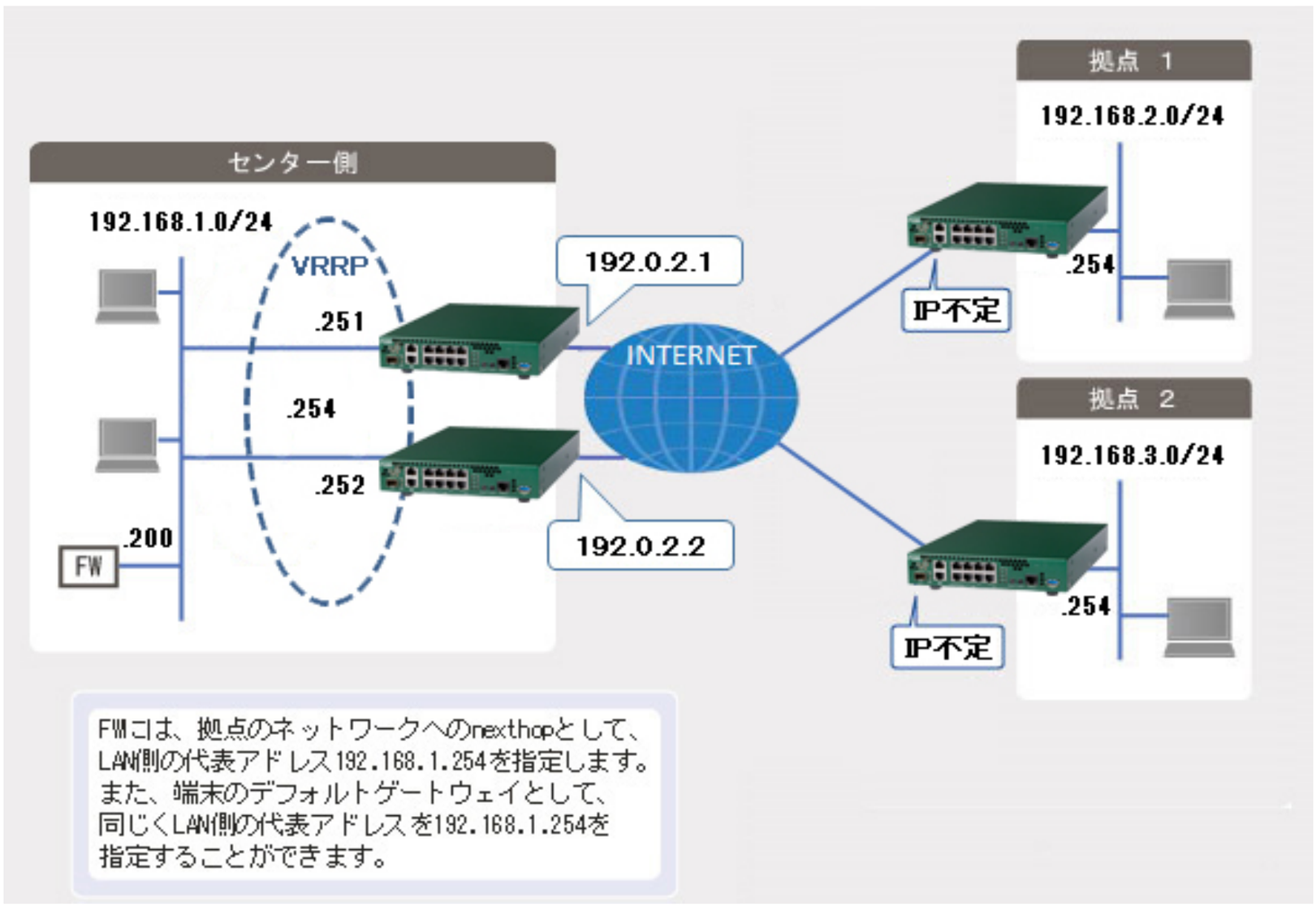
IPsec冗長：センタ側を機器および回線冗長～VRRPプライオリティ減算で切り替え

概要

センタ側機器はLAN側のFWをデフォルトゲートウェイとします。拠点からのVPN接続が行われると、拠点（VPNピア）の経路情報をWAN側インタフェース向けに登録して（トンネルルート機能）、VPNセッションを確立します。

センタ側機器はVRRP冗長構成とします。センタ側メインでWAN回線（PPPoE Tunnel）がダウンしたときには、VRRP Priorityを減算して、センタ側バックアップがVRRP Masterとなるような切り替えを行います。

拠点側機器はセンタ側メインのLAN宛にICMP監視（survey）を行い、ICMP監視状態がダウンとなった場合には、VPN経路をセンタ側バックアップに切り替えます。



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

センタ側メインの設定

	設定例（センタ）	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 0.0.0.0 192.168.1.200	Default経路(FW経由)
7	ip route 192.168.2.0 255.255.255.0 192.168.1.252 100	障害復旧時にセンタのSAが確立するまでの経路(拠点1)
8	ip route 192.168.2.0 255.255.255.0 tunnel 2	拠点1 LAN宛てStatic経路(IPsec Tunnel経由)
9	ip route 192.168.3.0 255.255.255.0 192.168.1.252 100	障害復旧時にセンタのSAが確立するまでの経路(拠点2)
10	ip route 192.168.3.0 255.255.255.0 tunnel 3	拠点2 LAN宛てStatic経路(IPsec Tunnel経由)
11	ip vrrp enable	VRRP 機能を有効
12	!	
13	track 10 ip host 192.0.2.1 reachability delay-up 30	PPPoEの状態とVRRPの状態を連携させる設定。PPPoEのアドレスを監視
14	!	
15	hostname CENTER1	
16	!	
17	crypto ipsec policy P2-POLICY	IPsecポリシー設定(Phase2 SAのパラメータを指定)
18	set pfs group14	
19	set security-association lifetime seconds 28800	
20	set security-association transform-keysize aes 256 256 256	
21	set security-association transform esp-aes esp-sha256-hmac	
22	set mtu 1454	
23	set ip df-bit 0	
24	set ip fragment post	
25	exit	
26	!	
27	crypto ipsec selector SELECTOR	セレクタ設定
28	src 1 ipv4 any	
29	dst 1 ipv4 any	
30	exit	
31	!	
32	hardware-fault-detection action reboot	ハードウェア故障を検出した際の動作を指定(装置再起動)
33	!	
34	logging level informational	
35	crypto isakmp keepalive	
36	crypto isakmp log sa	
37	crypto isakmp log session	
38	crypto isakmp log negotiation-fail	
39	crypto isakmp tunnel-route ip interface tunnel 1	VPNピアへの経路情報をTunnel 1向けに登録する設定(トンネルルート機能)
40	!	
41	crypto isakmp policy P1-POLICY	ISAKMPポリシー設定(Phase1 SAのパラメータを指定)
42	authentication pre-share	
43	encryption aes	
44	encryption-keysize aes 256 256 256	
45	group 14	
46	lifetime 86400	
47	hash sha-256	
48	initiate-mode aggressive	
49	exit	
50	!	
51	crypto isakmp profile PROF0001	拠点１へのISAKMPプロファイル設定
52	match identity user id-kyoten1	
53	local-address 192.0.2.1	
54	set isakmp-policy P1-POLICY	
55	set ipsec-policy P2-POLICY	
56	ike-version 1	
57	local-key SECRET-VPN	
58	exit	
59	!	
60	crypto isakmp profile PROF0002	拠点2へのISAKMPプロファイル設定
61	match identity user id-kyoten2	
62	local-address 192.0.2.1	
63	set isakmp-policy P1-POLICY	
64	set ipsec-policy P2-POLICY	
65	ike-version 1	
66	local-key SECRET-VPN	
67	exit	
68	!	
69	crypto map KYOTEN_1 ipsec-isakmp	拠点１へのCRYPTO MAP設定
70	match address SELECTOR	
71	set isakmp-profile PROF0001	
72	exit	
73	!	
74	crypto map KYOTEN_2 ipsec-isakmp	拠点2へのCRYPTO MAP設定
75	match address SELECTOR	
76	set isakmp-profile PROF0002	
77	exit	
78	!	
79	interface GigaEthernet 1/1	物理インタフェース(LAN側)
80	vlan-id 1	
81	bridge-group 1	
82	channel-group 1	
83	exit	
84	!	
85	interface GigaEthernet 2/1	物理インタフェース(WAN側 ※PPPoE)
86	vlan-id 2	
87	bridge-group 2	
88	pppoe enable	
89	exit	
90	!	

	設定例（センタ）	補足
91	interface Port-channel 1	論理インタフェース設定(LAN側 Giga 1/1と紐付け)
92	ip address 192.168.1.251 255.255.255.0	
93	mss 1300	
94	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
95	vrrp 1 priority 200	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。）
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	vrrp 1 track 10 decrement 110	トラッキングを有効にし、優先度から減算する設定
98	exit	
99	!	
100	interface Tunnel 1	Tunnelインタフェース設定(PPPoE)
101	description FLETS	
102	ip address 192.0.2.1 255.255.255.255	
103	ip access-group 100 in	
104	ip access-group 111 in	
105	ip access-group 121 out	
106	tunnel mode pppoe profile PPPOE_PROF	
107	pppoe interface gigaethernet 2/1	
108	exit	
109	!	
110	interface Tunnel 2	Tunnelインタフェース設定(IPsec Tunnel 拠点１向け)
111	tunnel mode ipsec map KYOTEN_1	
112	link-state sync-sa	
113	exit	
114	!	
115	interface Tunnel 3	Tunnelインタフェース設定(IPsec Tunnel 拠点２向け)
116	tunnel mode ipsec map KYOTEN_2	
117	link-state sync-sa	
118	exit	
119	!	
120	pppoe profile PPPOE_PROF	PPPoEプロファイル設定
121	account abc012@***.***.ne.jp xxxyyyzzz	
122	exit	
123	!	
124	end	

センタ側バックアップの設定

	設定例（センタ）	補足
1	access-list 100 permit udp any eq 500 192.0.2.2 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 192.0.2.2 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 0.0.0.0 192.168.1.200	Default経路(FW経由)
7	ip route 192.168.2.0 255.255.255.0 tunnel 2	拠点1 LAN宛てStatic経路(IPsec Tunnel経由)
8	ip route 192.168.3.0 255.255.255.0 tunnel 3	拠点2 LAN宛てStatic経路(IPsec Tunnel経由)
9	ip route 192.168.2.0 255.255.255.0 null 0 250	IPsec Tunnelダウン時に拠点1LAN宛てパケットを破棄する設定
10	ip route 192.168.3.0 255.255.255.0 null 0 250	IPsec Tunnelダウン時に拠点2LAN宛てパケットを破棄する設定
11	ip vrrp enable	VRRP 機能を有効
12	!	
13	hostname CENTER2	
14	!	
15	crypto ipsec policy P2-POLICY	IPsecポリシー設定(Phase2 SAのパラメータを指定)
16	set pfs group14	
17	set security-association lifetime seconds 28800	
18	set security-association transform-keysize aes 256 256 256	
19	set security-association transform esp-aes esp-sha256-hmac	
20	set mtu 1454	
21	set ip df-bit 0	
22	set ip fragment post	
23	exit	
24	!	
25	crypto ipsec selector SELECTOR	セレクタ設定
26	src 1 ipv4 any	
27	dst 1 ipv4 any	
28	exit	
29	!	
30	hardware-fault-detection action reboot	ハードウェア故障を検出した際の動作を指定(装置再起動)
31	!	
32	logging level informational	
33	crypto isakmp keepalive	
34	crypto isakmp log sa	
35	crypto isakmp log session	
36	crypto isakmp log negotiation-fail	
37	crypto isakmp tunnel-route ip interface tunnel 1	VPNピアへの経路情報をTunnel 1向けに登録する設定(トンネルルート機能)
38	!	
39	crypto isakmp policy P1-POLICY	ISAKMPポリシー設定(Phase1 SAのパラメータを指定)
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 PROF0001	拠点１へのISAKMPプロファイル設定
50	match identity user id-kyoten1	
51	local-address 192.0.2.2	
52	set isakmp-policy P1-POLICY	
53	set ipsec-policy P2-POLICY	
54	ike-version 1	
55	local-key SECRET-VPN	
56	exit	
57	!	

	設定例（センタ）	補足
58	crypto isakmp profile PROF0002	拠点2へのISAKMPプロファイル設定
59	match identity user id-kyoten2	
60	local-address 192.0.2.2	
61	set isakmp-policy P1-POLICY	
62	set ipsec-policy P2-POLICY	
63	ike-version 1	
64	local-key SECRET-VPN	
65	exit	
66	!	
67	crypto map KYOTEN_1 ipsec-isakmp	拠点１へのCRYPTO MAP設定
68	match address SELECTOR	
69	set isakmp-profile PROF0001	
70	exit	
71	!	
72	crypto map KYOTEN_2 ipsec-isakmp	拠点2へのCRYPTO MAP設定
73	match address SELECTOR	
74	set isakmp-profile PROF0002	
75	exit	
76	!	
77	interface GigaEthernet 1/1	物理インタフェース(LAN側)
78	vlan-id 1	
79	bridge-group 1	
80	channel-group 1	
81	exit	
82	!	
83	interface GigaEthernet 2/1	物理インタフェース(WAN側 ※PPPoE)
84	vlan-id 2	
85	bridge-group 2	
86	pppoe enable	
87	exit	
88	!	
89	interface Port-channel 1	論理インタフェース設定(LAN側 Giga 1/1と紐付け)
90	ip address 192.168.1.252 255.255.255.0	
91	mss 1300	
92	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
93	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。）
94	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。
95	exit	
96	!	
97	interface Tunnel 1	Tunnelインタフェース設定(PPPoE)
98	description FLETS	
99	ip address 192.0.2.2 255.255.255.255	
100	ip access-group 100 in	
101	ip access-group 111 in	
102	ip access-group 121 out	
103	tunnel mode pppoe profile PPPOE_PROF	
104	pppoe interface gigaethernet 2/1	
105	exit	
106	!	
107	interface Tunnel 2	Tunnelインタフェース設定(IPsec Tunnel 拠点1向け)
108	tunnel mode ipsec map KYOTEN_1	
109	link-state sync-sa	
110	exit	
111	!	
112	interface Tunnel 3	Tunnelインタフェース設定(IPsec Tunnel 拠点2向け)
113	tunnel mode ipsec map KYOTEN_2	
114	link-state sync-sa	
115	exit	
116	!	
117	pppoe profile PPPOE_PROF	PPPoEプロファイル設定
118	account abc123@***.***.ne.jp yyyxxxzzz	
119	exit	
120	!	
121	end	

拠点1の設定

	設定例（拠点）	補足
1	access-list 100 permit udp 192.0.2.1 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 50 192.0.2.1 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 100 permit udp 192.0.2.2 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 100 permit 50 192.0.2.2 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 0.0.0.0 0.0.0.0 tunnel 1	Default経路(PPPoE経由)
9	ip route 192.168.1.0 255.255.255.0 null 0 150	IPsec Tunnelダウン時にセンタLAN宛てパケットを破棄する設定
10	ip route 192.168.1.0 255.255.255.0 tunnel 2 survey name t2_ICMP	センタLAN宛てメイン経路(IPsec Tunnel経由)、ICMP監視結果と連動させる
11	ip route 192.168.1.0 255.255.255.0 tunnel 3 100	センタLAN宛てバックアップ経路(IPsec Tunnel経由)、ディスタンス100を設定してメイン経路よりも優先度を低くする
12	ip nat list 1 192.168.2.0 0.0.0.255	NAT変換対象とする送信元アドレスを登録
13	!	
14	survey 192.168.1.251 name t2_ICMP survey-map ICMP-Kanshi source port-channel 1 nexthop tunnel 2 interworking	Tunnel 2経由でセンタ側のLAN側IPアドレスをICMP監視して、"interworking"を指定することで、ICMP監視結果とTunnel 2のup/downを同期させる
15	!	
16	survey-map ICMP-Kanshi	survey-map設定(ICMP監視パラメータを指定)
17	retry 2 interval 10000	
18	frequency every 10000	
19	stability 2 interval 10000	
20	exit	
21	!	
22	hostname KYOTEN1	
23	!	
24	crypto ipsec policy P2-POLICY	IPsecポリシー設定(Phase2 SAのパラメータを指定)
25	set pfs group14	
26	set security-association always-up	
27	set security-association lifetime seconds 28800	
28	set security-association transform-keysize aes 256 256 256	
29	set security-association transform esp-aes esp-sha256-hmac	
30	set mtu 1454	
31	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。
32	set ip df-bit 0	
33	set ip fragment post	
34	exit	
35	!	
36	crypto ipsec selector SELECTOR	セレクタ設定
37	src 1 ipv4 any	
38	dst 1 ipv4 any	
39	exit	
40	!	
41	hardware-fault-detection action reboot	ハードウェア故障を検出した際の動作を指定(装置再起動)
42	!	
43	logging level informational	
44	crypto isakmp keepalive	
45	crypto isakmp log sa	
46	crypto isakmp log session	
47	crypto isakmp log negotiation-fail	
48	!	
49	crypto isakmp policy P1-POLICY	ISAKMPポリシー設定(Phase1 SAのパラメータを指定)
50	authentication pre-share	
51	encryption aes	
52	encryption-keysize aes 256 256 256	
53	group 14	
54	lifetime 86400	
55	hash sha-256	
56	initiate-mode aggressive	
57	exit	
58	!	
59	crypto isakmp profile PROF0001	センタ側メインへのISAKMPプロファイル設定
60	self-identity user-fqdn id-kyoten1	
61	set isakmp-policy P1-POLICY	
62	set ipsec-policy P2-POLICY	
63	set peer 192.0.2.1	
64	ike-version 1	
65	local-key SECRET-VPN	
66	exit	
67	!	
68	crypto isakmp profile PROF0002	センタ側バックアップへのISAKMPプロファイル設定
69	self-identity user-fqdn id-kyoten1	
70	set isakmp-policy P1-POLICY	
71	set ipsec-policy P2-POLICY	
72	set peer 192.0.2.2	
73	ike-version 1	
74	local-key SECRET-VPN	
75	exit	
76	!	
77	crypto map CENTER ipsec-isakmp	センタ側メインへのCRYPTO MAP設定
78	match address SELECTOR	
79	set isakmp-profile PROF0001	
80	exit	
81	!	
82	crypto map CENTER_BK ipsec-isakmp	センタ側バックアップへのCRYPTO MAP設定
83	match address SELECTOR	
84	set isakmp-profile PROF0002	
85	exit	
86	!	

	設定例（拠点）	補足
87	interface GigaEthernet 1/1	物理インタフェース(LAN側)
88	vlan-id 1	
89	bridge-group 1	
90	channel-group 1	
91	exit	
92	!	
93	interface GigaEthernet 2/1	物理インタフェース(WAN側 ※PPPoE)
94	vlan-id 2	
95	bridge-group 2	
96	pppoe enable	
97	exit	
98	!	
99	interface Port-channel 1	論理インタフェース設定(LAN側 Giga 1/1と紐付け)
100	ip address 192.168.2.254 255.255.255.0	
101	mss 1300	
102	exit	
103	!	
104	interface Tunnel 1	Tunnelインタフェース設定(PPPoE)
105	description FLETS	
106	ip access-group 100 in	
107	ip access-group 111 in	
108	ip access-group 121 out	
109	ip nat inside source list 1 interface	
110	tunnel mode pppoe profile PPPOE_PROF	
111	pppoe interface gigaethernet 2/1	
112	exit	
113	!	
114	interface Tunnel 2	Tunnelインタフェース設定(IPsec Tunnel センタ側メイン向け) ※ICMP監視結果と連動させるため、link-state sync-saは設定しない
115	tunnel mode ipsec map CENTER	
116	exit	
117	!	
118	interface Tunnel 3	Tunnelインタフェース設定(IPsec Tunnel センタ側バックアップ向け)
119	tunnel mode ipsec map CENTER_BK	
120	link-state sync-sa	
121	exit	
122	!	
123	pppoe profile PPPOE_PROF	PPPoEプロファイル設定
124	account abc345@***.***.ne.jp zzzyyyxxx	
125	exit	
126	!	
127	end	

拠点2の設定

	設定例（拠点）	補足
1	access-list 100 permit udp 192.0.2.1 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 50 192.0.2.1 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 100 permit udp 192.0.2.2 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 100 permit 50 192.0.2.2 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 0.0.0.0 0.0.0.0 tunnel 1	Default経路(PPPoE経由)
9	ip route 192.168.1.0 255.255.255.0 null 0 150	IPsec Tunnelダウン時にセンタLAN宛てパケットを破棄する設定
10	ip route 192.168.1.0 255.255.255.0 tunnel 2 survey name t2_ICMP	センタLAN宛てメイン経路(IPsec Tunnel経由)、ICMP監視結果と連動させる
11	ip route 192.168.1.0 255.255.255.0 tunnel 3 100	センタLAN宛てバックアップ経路(IPsec Tunnel経由)、ディスタンス100を設定してメイン経路よりも優先度を低くする
12	ip nat list 1 192.168.3.0 0.0.0.255	NAT変換対象とする送信元アドレスを登録
13	!	
14	survey 192.168.1.251 name t2_ICMP survey-map ICMP-Kanshi source port-channel 1 nexthop tunnel 2 interworking	Tunnel 2経由でセンタ側のLAN側IPアドレスをICMP監視して、"interworking"を指定することで、ICMP監視結果とTunnel 2のup/downを同期させる
15	!	
16	survey-map ICMP-Kanshi	survey-map設定(ICMP監視パラメータを指定)
17	retry 2 interval 10000	
18	frequency every 10000	
19	stability 2 interval 10000	
20	exit	
21	!	
22	hostname KYOTEN2	
23	!	
24	crypto ipsec policy P2-POLICY	IPsecポリシー設定(Phase2 SAのパラメータを指定)
25	set pfs group14	
26	set security-association always-up	
27	set security-association lifetime seconds 28800	
28	set security-association transform-keysize aes 256 256 256	
29	set security-association transform esp-aes esp-sha256-hmac	
30	set mtu 1454	
31	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。
32	set ip df-bit 0	
33	set ip fragment post	
34	exit	
35	!	
36	crypto ipsec selector SELECTOR	セレクタ設定
37	src 1 ipv4 any	
38	dst 1 ipv4 any	
39	exit	
40	!	
41	hardware-fault-detection action reboot	ハードウェア故障を検出した際の動作を指定(装置再起動)
42	!	

	設定例（拠点）	補足
43	logging level informational	
44	crypto isakmp keepalive	
45	crypto isakmp log sa	
46	crypto isakmp log session	
47	crypto isakmp log negotiation-fail	
48	!	
49	crypto isakmp policy P1-POLICY	ISAKMPポリシー設定(Phase1 SAのパラメータを指定)
50	authentication pre-share	
51	encryption aes	
52	encryption-keysize aes 256 256 256	
53	group 14	
54	lifetime 86400	
55	hash sha-256	
56	initiate-mode aggressive	
57	exit	
58	!	
59	crypto isakmp profile PROF0001	センタ側メインへのISAKMPプロファイル設定
60	self-identity user-fqdn id-kyoten2	
61	set isakmp-policy P1-POLICY	
62	set ipsec-policy P2-POLICY	
63	set peer 192.0.2.1	
64	ike-version 1	
65	local-key SECRET-VPN	
66	exit	
67	!	
68	crypto isakmp profile PROF0002	センタ側バックアップへのISAKMPプロファイル設定
69	self-identity user-fqdn id-kyoten2	
70	set isakmp-policy P1-POLICY	
71	set ipsec-policy P2-POLICY	
72	set peer 192.0.2.2	
73	ike-version 1	
74	local-key SECRET-VPN	
75	exit	
76	!	
77	crypto map CENTER ipsec-isakmp	センタ側メインへのCRYPTO MAP設定
78	match address SELECTOR	
79	set isakmp-profile PROF0001	
80	exit	
81	!	
82	crypto map CENTER_BK ipsec-isakmp	センタ側バックアップへのCRYPTO MAP設定
83	match address SELECTOR	
84	set isakmp-profile PROF0002	
85	exit	
86	!	
87	interface GigaEthernet 1/1	物理インタフェース(LAN側)
88	vlan-id 1	
89	bridge-group 1	
90	channel-group 1	
91	exit	
92	!	
93	interface GigaEthernet 2/1	物理インタフェース(WAN側 ※PPPoE)
94	vlan-id 2	
95	bridge-group 2	
96	pppoe enable	
97	exit	
98	!	
99	interface Port-channel 1	論理インタフェース設定(LAN側 Giga 1/1と紐付け)
100	ip address 192.168.3.254 255.255.255.0	
101	mss 1300	
102	exit	
103	!	
104	interface Tunnel 1	Tunnelインタフェース設定(PPPoE)
105	description FLETS	
106	ip access-group 100 in	
107	ip access-group 111 in	
108	ip access-group 121 out	
109	ip nat inside source list 1 interface	
110	tunnel mode pppoe profile PPPOE_PROF	
111	pppoe interface gigaethernet 2/1	
112	exit	
113	!	
114	interface Tunnel 2	Tunnelインタフェース設定(IPsec Tunnel センタ側メイン向け) ※ICMP監視結果と連動させるため、link-state sync-saは設定しない
115	tunnel mode ipsec map CENTER	
116	exit	
117	!	
118	interface Tunnel 3	Tunnelインタフェース設定(IPsec Tunnel センタ側バックアップ向け)
119	tunnel mode ipsec map CENTER_BK	
120	link-state sync-sa	
121	exit	
122	!	
123	pppoe profile PPPOE_PROF	PPPoEプロファイル設定
124	account abc678@***.***.ne.jp yyyzzzxxx	
125	exit	
126	!	
127	end	