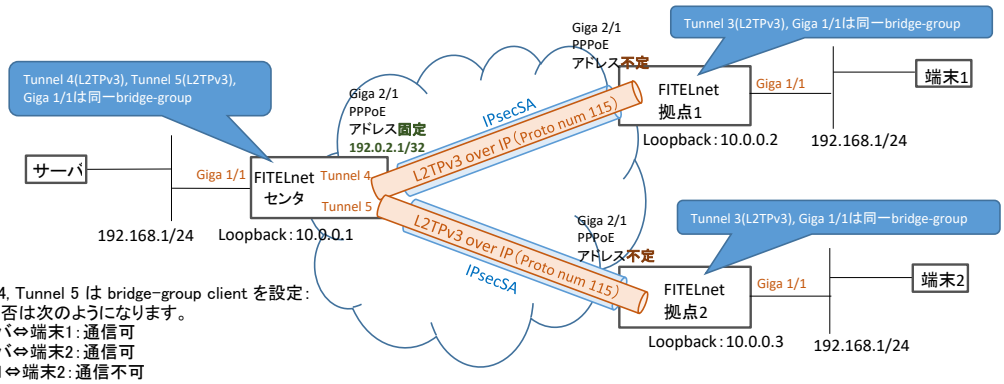
設定例

拠点間を L2TPv3 機能で接続する

概要

L2TPv3機能を使用して、複数拠点のLANからセンタのLANにアクセスするための設定例です。
・本設定例では、センタにbridge-group clientを設定して、拠点1-拠点2間のトンネル折り返し通信を遮断しています。



※Tunnel 4, Tunnel 5 は bridge-group client を設定:
通信可否は次のようになります。
サーバ⇔端末1:通信可
サーバ⇔端末2:通信可
端末1⇔端末2:通信不可

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

パラメータ設定例

センタ側FITELnet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 tunnel 1	Default経路(PPPoE経由)
7	ip route 10.0.0.2 255.255.255.255 tunnel 2	L2TPv3対向拠点1のIPアドレス(Loopback)宛への経路(IPsec Tunnel経由)
8	ip route 10.0.0.3 255.255.255.255 tunnel 3	L2TPv3対向拠点2のIPアドレス(Loopback)宛への経路(IPsec Tunnel経由)
9	!	
10	hostname CENTER	
11	!	
12	crypto ipsec policy P2-POLICY	IPSECポリシーの設定
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 SELECTOR	VPNセレクタの設定
23	src 1 ipv4 any	
24	dst 1 ipv4 any	
25	exit	
26	!	
27	crypto isakmp keepalive	KeepAlive機能として使用するDPDの設定
28	logging level informational	各種の詳細なログを出力する設定
29	crypto isakmp log sa	SA確立／解放のログを出力する設定
30	crypto isakmp log session	セッション確立／ 解放のログを出力する設定
31	crypto isakmp log negotiation-fail	IKEネゴシ エーション失敗のログを出力する設定
32	l2tpv3 log session	L2TPv3のログを出力する設定
33	!	
34	crypto isakmp policy P1-POLICY	ISAKMP ポリシーの設定
35	authentication pre-share	
36	encryption aes	
37	encryption-keysize aes 256 256 256	
38	group 14	
39	lifetime 86400	
40	hash sha	
41	initiate-mode aggressive	
42	exit	

43	!	
44	crypto isakmp profile PROF0001	ISAKMPプロファイルの設定（拠点1）
45	match identity user id-kyoten1	
46	local-address 192.0.2.1	
47	set isakmp-policy P1-POLICY	
48	set ipsec-policy P2-POLICY	
49	ike-version 1	
50	local-key SECRET-VPN	
51	exit	
52	!	
53	crypto isakmp profile PROF0002	ISAKMPプロファイルの設定（拠点2）
54	match identity user id-kyoten2	
55	local-address 192.0.2.1	
56	set isakmp-policy P1-POLICY	
57	set ipsec-policy P2-POLICY	
58	ike-version 1	
59	local-key SECRET-VPN	
60	exit	
61	!	
62	crypto map KYOTEN1 ipsec-isakmp	拠点1のVPNピアとのセレクタ情報のエントリ
63	match address SELECTOR	
64	set isakmp-profile PROF0001	
65	exit	
66	!	
67	crypto map KYOTEN2 ipsec-isakmp	拠点2のVPNピアとのセレクタ情報のエントリ
68	match address SELECTOR	
69	set isakmp-profile PROF0002	
70	exit	
71	!	
72	interface GigaEthernet 1/1	GigaEthernet（1/1）インタフェースに、L2TPv3トンネルをリンク付け
73	vlan-id 1	
74	bridge-group 1	ブリッジグループを指定：L2TPv3のTunnelインターフェースで使用する bridge-groupと合わせる
75	exit	
76	!	
77	interface GigaEthernet 2/1	PPPoE 通信で使用する物理インタフェースの設定
78	vlan-id 2	
79	bridge-group 2	
80	pppoe enable	
81	exit	
82	!	
83	interface Loopback 1	Loopback インタフェースの設定
84	ip address 10.0.0.1	
85	exit	
86	!	
87	interface Tunnel 1	Tunnel インタフェース（PPPoE）の設定
88	description FLETS	
89	ip address 192.0.2.1 255.255.255.255	
90	ip access-group 100 in	
91	ip access-group 111 in	
92	ip access-group 121 out	
93	tunnel mode pppoe profile PPPOE_PROF	
94	pppoe interface gigaethernet 2/1	
95	exit	
96	!	
97	interface Tunnel 2	拠点1向けTunnel インタフェース（IPsec）の設定
98	tunnel mode ipsec map KYOTEN1	
99	exit	
100	!	
101	interface Tunnel 3	拠点2向けTunnel インタフェース（IPsec）の設定
102	tunnel mode ipsec map KYOTEN2	
103	exit	
104	!	
105	interface Tunnel 4	拠点1向けTunnel インタフェース（L2TPv3）の設定
106	tunnel mode l2tpv3 pseudowire L2TPv3_kyoten1	L2TPv3 PSEUDOWIREプロファイルの設定
107	bridge-group 1 client	ブリッジグループを指定：LAN側インタフェース（GigaEthernet 1/1）で使用する bridge-groupと合わせる 拠点1-拠点2間で通信行わないようにするためにclientを指定
108	exit	
109	interface Tunnel 5	拠点2向けTunnel インタフェース（L2TPv3）の設定
110	tunnel mode l2tpv3 pseudowire L2TPv3_kyoten2	L2TPv3 PSEUDOWIREプロファイルの設定
111	bridge-group 1 client	ブリッジグループを指定：LAN側インタフェース（GigaEthernet 1/1）で使用する bridge-groupと合わせる 拠点1-拠点2間で通信行わないようにするためにclientを指定
112	exit	
113	!	
114	l2tpv3 tunnel-profile L2TPv3_PROF_kyoten1	拠点1向けL2TPv3プロファイルの設定
115	mode l2tpv3	RFC3931準拠の設定
116	tunnel source 10.0.0.1	L2TPv3トンネルを確立する自装置（Loopback）IPアドレスの設定
117	tunnel destination 10.0.0.2	L2TPv3の通信をする拠点1側装置（Loopback）IPアドレスの設定
118	tunnel protection ipsec tunnel 2	L2TPv3 over IPsec環境下で、L2TPv3 tunnel インタフェースと紐付ける IPsec tunnelインタフェースの設定
119	hostname local CENTER	自装置から送信されるHost Name AVPに含まれるホスト名の設定
120	hostname remote KYOTEN1	拠点1側装置から受信したHost Name AVPの値をチェックする設定
121	hello interval 10	L2TPv3のkeepaliveで使用するHelloメッセージの送信間隔の設定
122	exit	
123	!	
124	l2tpv3 tunnel-profile L2TPv3_PROF_kyoten2	拠点2向けL2TPv3プロファイルの設定
125	mode l2tpv3	RFC3931準拠の設定
126	tunnel source 10.0.0.1	L2TPv3トンネルを確立する自装置（Loopback）IPアドレスの設定
127	tunnel destination 10.0.0.3	L2TPv3の通信をする拠点2側装置（Loopback）IPアドレスの設定
128	tunnel protection ipsec tunnel 3	L2TPv3 over IPsec環境下で、L2TPv3 tunnel インタフェースと紐付ける IPsec tunnelインタフェースの設定
129	hostname local CENTER	自装置から送信されるHost Name AVPに含まれるホスト名の設定
130	hostname remote KYOTEN2	拠点2側装置から受信したHost Name AVPの値をチェックする設定
131	hello interval 10	L2TPv3のkeepaliveで使用するHelloメッセージの送信間隔の設定
132	exit	
133	!	
134	l2tpv3 pseudowire L2TPv3_kyoten1	拠点1向けL2TPv3 Pseudowireの設定
135	set profile L2TPv3_PROF_kyoten1	拠点1向けL2TPv3 PseudowireとL2TPv3プロファイルのリンク付け

136	remote-end-id ascii ID_center_kyoten1	セッションを識別するためのIDの設定 （センタと拠点1で同じ値を設定する必要があります）
137	exit	
138	!	
139	l2tpv3 pseudowire L2TPv3_kyoten2	拠点2向けL2TPv3 Pseudowireの設定
140	set profile L2TPv3_PROF_kyoten2	拠点2向けL2TPv3 PseudowireとL2TPv3プロファイルのリンク付け
141	remote-end-id ascii ID_center_kyoten2	セッションを識別するためのIDの設定 （センタと拠点2で同じ値を設定する必要があります）
142	exit	
143	!	
144	pppoe profile PPPOE_PROF	PPPoEの設定
145	account abc012@***.***.ne.jp xxxyyyzzz	
146	exit	
147	!	
148	end	

拠点側FITELnetの設定（拠点1）

	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 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	Default経路(PPPoE経由)
7	ip route 10.0.0.1 255.255.255.255 tunnel 2	L2TPv3対向センタ機のIPアドレス(Loopback)宛への経路(IPsec Tunnel経由)
8	!	
9	hostname KYOTEN1	
10	!	
11	crypto ipsec policy P2-POLICY	IPSECポリシーの設定
12	set pfs group14	
13	set security-association always-up	
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 SELECTOR	VPNセレクタの設定
23	src 1 ipv4 any	
24	dst 1 ipv4 any	
25	exit	
26	!	
27	crypto isakmp keepalive	KeepAlive機能として使用するDPDの設定
28	logging level informational	各種の詳細なログを出力する設定
29	crypto isakmp log sa	SA確立／解放のログを出力する設定
30	crypto isakmp log session	セッション確立／ 解放のログを出力する設定
31	crypto isakmp log negotiation-fail	IKEネゴシ エーション失敗のログを出力する設定
32	l2tpv3 log session	L2TPv3のログを出力する設定
33	!	
34	crypto isakmp policy P1-POLICY	ISAKMP ポリシーの設定
35	authentication pre-share	
36	encryption aes	
37	encryption-keysize aes 256 256 256	
38	group 14	
39	lifetime 86400	
40	hash sha	
41	initiate-mode aggressive	
42	exit	
43	!	
44	crypto isakmp profile PROF0001	ISAKMPプロファイルの設定
45	self-identity user-fqdn id-kyoten1	
46	set peer 192.0.2.1	
47	set isakmp-policy P1-POLICY	
48	set ipsec-policy P2-POLICY	
49	ike-version 1	
50	local-key SECRET-VPN	
51	exit	
52	!	
53	crypto map CENTER ipsec-isakmp	VPNピアとのセレクタ情報のエントリ
54	match address SELECTOR	
55	set isakmp-profile PROF0001	
56	exit	
57	!	
58	interface GigaEthernet 1/1	GigaEthernet（1/1）インタフェースに、L2TPv3トンネルをリンク付け
59	vlan-id 1	
60	bridge-group 1	ブリッジグループを指定：L2TPv3のTunnelインターフェースで使用する bridge-groupと合わせる
61	exit	
62	!	
63	interface GigaEthernet 2/1	PPPoE 通信で使用する物理インタフェースの設定
64	vlan-id 2	
65	bridge-group 2	
66	pppoe enable	
67	exit	
68	!	
69	interface Loopback 1	Loopback インタフェースの設定
70	ip address 10.0.0.2	
71	exit	
72	!	
73	interface Tunnel 1	Tunnel インタフェース（PPPoE）の設定
74	description FLETS	
75	ip access-group 100 in	
76	ip access-group 111 in	
77	ip access-group 121 out	
78	tunnel mode pppoe profile PPPOE_PROF	
79	pppoe interface gigaethernet 2/1	
80	exit	
81	!	
82	interface Tunnel 2	センタ向けTunnel インタフェース（IPsec）の設定
83	tunnel mode ipsec map CENTER	
84	exit	
85	!	
86	interface Tunnel 3	センタ向けTunnel インタフェース（L2TPv3）の設定
87	tunnel mode l2tpv3 pseudowire L2TPv3_center	L2TPv3 PSEUDOWIREプロファイルの設定
88	bridge-group 1	ブリッジグループを指定：LAN側インタフェース（GigaEthernet 1/1）で使用する bridge-groupと合わせる
89	exit	
90	!	
91	l2tpv3 tunnel-profile L2TPv3_PROF_center	センタ向けL2TPv3プロファイルの設定
92	mode l2tpv3	RFC3931準拠の設定
93	tunnel source 10.0.0.2	L2TPv3トンネルを確立する自装置（Loopback）IPアドレスの設定
94	tunnel destination 10.0.0.1	L2TPv3の通信をするセンタ側装置（Loopback）IPアドレスの設定

	設定例(拠点)	補足
95	tunnel protection ipsec tunnel 2	L2TPv3 over IPsec環境下で、L2TPv3 tunnel インタフェースと紐付ける IPsec tunnelインタフェースの設定
96	hostname local KYOTEN1	自装置から送信されるHost Name AVPに含まれるホスト名の設定
97	hostname remote CENTER	センタ側装置から受信したHost Name AVPの値をチェックする設定
98	hello interval 10	L2TPv3のkeepaliveで使用するHelloメッセージの送信間隔の設定
99	exit	
100	!	
101	l2tpv3 pseudowire L2TPv3_center	センタ向けL2TPv3 Pseudowireの設定
102	set profile L2TPv3_PROF_center	センタ向けL2TPv3 PseudowireとL2TPv3プロファイルのリンク付け
103	remote-end-id ascii ID_center_kyoten1	セッションを識別するためのIDの設定 (センタと拠点1で同じ値を設定する必要があります)
104	always-up	常にL2TPv3セッションを確立しておく設定
105	exit	
106		
107	pppoe profile PPPOE_PROF	PPPoEの設定
108	account abc345@***.***.ne.jp zzzyyyxxx	
109	exit	
110	!	
111	end	

拠点側FITELnetの設定(拠点2)

	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 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	Default経路(PPPoE経由)
7	ip route 10.0.0.1 255.255.255.255 tunnel 2	L2TPv3対向センタ機のIPアドレス(Loopback)宛への経路(IPsec Tunnel経由)
8	!	
9	hostname KYOTEN2	
10	!	
11	crypto ipsec policy P2-POLICY	IPSECポリシーの設定
12	set pfs group14	
13	set security-association always-up	
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 SELECTOR	VPNセレクタの設定
23	src 1 ipv4 any	
24	dst 1 ipv4 any	
25	exit	
26	!	
27	crypto isakmp keepalive	KeepAlive機能として使用するDPDの設定
28	logging level informational	各種の詳細なログを出力する設定
29	crypto isakmp log sa	SA確立／解放のログを出力する設定
30	crypto isakmp log session	セッション確立／ 解放のログを出力する設定
31	crypto isakmp log negotiation-fail	IKEネゴシ エーション失敗のログを出力する設定
32	l2tpv3 log session	L2TPv3のログを出力する設定
33	!	
34	crypto isakmp policy P1-POLICY	ISAKMP ポリシーの設定
35	authentication pre-share	
36	encryption aes	
37	encryption-keysize aes 256 256 256	
38	group 14	
39	lifetime 86400	
40	hash sha	
41	initiate-mode aggressive	
42	exit	
43	!	
44	crypto isakmp profile PROF0001	ISAKMPプロファイルの設定
45	self-identity user-fqdn id-kyoten2	
46	set peer 192.0.2.1	
47	set isakmp-policy P1-POLICY	
48	set ipsec-policy P2-POLICY	
49	ike-version 1	
50	local-key SECRET-VPN	
51	exit	
52	!	
53	crypto map CENTER ipsec-isakmp	VPNピアとのセレクタ情報のエントリ
54	match address SELECTOR	
55	set isakmp-profile PROF0001	
56	exit	
57	!	
58	interface GigaEthernet 1/1	GigaEthernet(1/1)インタフェースに、L2TPv3トンネルをリンク付け
59	vlan-id 1	
60	bridge-group 1	ブリッジグループを指定:L2TPv3のTunnelインターフェースで使用する bridge-groupと合わせる
61	exit	
62	!	
63	interface GigaEthernet 2/1	PPPoE 通信で使用する物理インタフェースの設定
64	vlan-id 2	
65	bridge-group 2	
66	pppoe enable	
67	exit	
68	!	
69	interface Loopback 1	Loopback インタフェースの設定
70	ip address 10.0.0.3	
71	exit	
72	!	
73	interface Tunnel 1	Tunnel インタフェース(PPPoE)の設定

	設定例(拠点)	補足
74	description FLETS	
75	ip access-group 100 in	
76	ip access-group 111 in	
77	ip access-group 121 out	
78	tunnel mode pppoe profile PPPOE_PROF	
79	pppoe interface gigaethernet 2/1	
80	exit	
81	!	
82	interface Tunnel 2	センタ向けTunnel インタフェース(IPsec)の設定
83	tunnel mode ipsec map CENTER	
84	exit	
85	!	
86	interface Tunnel 3	センタ向けTunnel インタフェース(L2TPv3)の設定
87	tunnel mode l2tpv3 pseudowire L2TPv3_center	L2TPv3 PSEUDOWIREプロファイルの設定
88	bridge-group 1	ブリッジグループを指定:LAN側インタフェース(GigaEthernet 1/1)で使用する bridge-groupと合わせる
89	exit	
90	!	
91	l2tpv3 tunnel-profile L2TPv3_PROF_center	センタ向けL2TPv3プロファイルの設定
92	mode l2tpv3	RFC3931準拠の設定
93	tunnel source 10.0.0.3	L2TPv3トンネルを確立する自装置(Loopback)IPアドレスの設定
94	tunnel destination 10.0.0.1	L2TPv3の通信をするセンタ側装置(Loopback)IPアドレスの設定
95	tunnel protection ipsec tunnel 2	L2TPv3 over IPsec環境下で、L2TPv3 tunnel インタフェースと紐付ける IPsec tunnelインタフェースの設定
96	hostname local KYOTEN2	自装置から送信されるHost Name AVPに含まれるホスト名の設定
97	hostname remote CENTER	センタ側装置から受信したHost Name AVPの値をチェックする設定
98	hello interval 10	L2TPv3のkeepaliveで使用するHelloメッセージの送信間隔の設定
99	exit	
100	!	
101	l2tpv3 pseudowire L2TPv3_center	センタ向けL2TPv3 Pseudowireの設定
102	set profile L2TPv3_PROF_center	センタ向けL2TPv3 PseudowireとL2TPv3プロファイルのリンク付け
103	remote-end-id ascii ID_center_kyoten2	セッションを識別するためのIDの設定 (センタと拠点2で同じ値を設定する必要があります)
104	always-up	常にL2TPv3セッションを確立しておく設定
105	exit	
106	!	
107	pppoe profile PPPOE_PROF	PPPoEの設定
108	account abc678@***.***.ne.jp yyyzzzxxx	
109	exit	
110	!	
111	end	