設定例

拠点間を EtherIP 機能で接続する：vlan-id anyを使用

概要

EtherIPとvlan-id anyを使用して、拠点の複数のネットワークから、センタのサーバに接続するための設定例です。

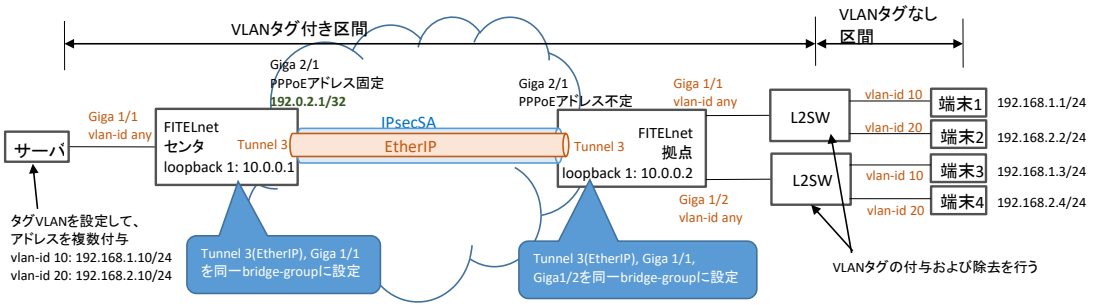
・vlan-id any設定を行ったGigaインタフェースでは、VLANタグを透過します（VLANタグの付与/除去を行いません）。端末でVLANタグ付きフレームを扱わない場合は下記構成図のようにL2SWを設置して、L2SWでVLANタグの付与/除去を行うことが必要です。

・VLANタグ付きフレームを扱わない端末をFITELnetに直結する場合は、Gigaインタフェースにvlan-id anyではなく特定のVLAN-IDを指定、かつ tagging transparentを指定するようにしてください。FITELnetが当該Gigaインタフェースで受信したフレームを他のインタフェースに転送時にVLANタグを付与、かつ当該Gigaインタフェースから送信するフレームからVLANタグを除去します。

・FITELnetのLANインタフェース（Giga1/1～1/8）にて、同一のVLAN-IDの折り返し中継は可能ですが、異なるVLAN-IDの折り返し中継はできません。

・同一ブリッジグループに異なる複数のVLAN-IDを設定した場合やvlan-id anyを設定した場合の中継動作については、下記機能説明書のVLAN機能の章（1bridge複数VLAN機能）をご参照ください。
https://www.furukawa.co.jp/fitelnet/f/man/220/pdf/kinou.pdf

・本設定例では、基本設定モードの vlan-id any <VLAN-ID値> コマンドでで対象とするVLAN-ID値を指定します。対象とするVLAN-IDを指定しない場合は、1-4094の全VLAN-IDが対象になりますが、設定反映に数分程度の時間を要します。



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-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

センタ側FITELnetの設定

	設定例	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	EtherIP対向装置のIPアドレス(Loopback)宛への経路(IPsec Tunnel経由)
8	!	
9	hostname CENTER	
10	!	
11	crypto ipsec policy P2-POLICY	IPSECポリシーの設定
12	set pfs group14	
13	set security-association lifetime seconds 28800	
14	set security-association transform-keysize aes 256 256 256	
15	set security-association transform esp-aes esp-sha-hmac	
16	set mtu 1454	
17	set ip df-bit 0	
18	set ip fragment post	
19	exit	
20	!	
21	crypto ipsec selector SELECTOR	VPNセレクタの設定
22	src 1 ipv4 any	
23	dst 1 ipv4 any	
24	exit	
25	!	
26	crypto isakmp keepalive	KeepAlive機能として使用するDPDの設定
27	logging level informational	VPN通信動作中の詳細なログを残す設定
28	crypto isakmp log sa	
29	crypto isakmp log session	
30	crypto isakmp log negotiation-fail	
31	!	

All Rights Reserved, Copyright(C) FURUKAWA ELECTRIC CO., LTD. 2020

	設定例	補足
32	crypto isakmp policy P1-POLICY	ISAKMP ポリシーの設定
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プロファイルの設定
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 KYOTEN ipsec-isakmp	拠点のVPNピアとのセレクタ情報のエントリー
52	match address SELECTOR	
53	set isakmp-profile PROF0001	
54	exit	
55	!	
56	vlan-id any 10 20	VLANーIDをANY(1～4094)に指定。 ※対象とするVLAN-IDを基本設定モードのvlan-id anyコマンドで指定可能。指定しない場合は1-4094の全VLAN-IDが対象になるが、設定反映に時間を要する。
57	!	
58	interface GigaEthernet 1/1	GigaEthernet(1/1)インタフェースに、EtherIPトンネルをリンク付け
59	vlan-id any	VLANーIDをANY(1～4094)に指定。 ※対象とするVLAN-IDを基本設定モードのvlan-id anyコマンドで指定可能。指定しない場合は1-4094の全VLAN-IDが対象になるが、設定反映に時間を要する。
60	bridge-group 1	ブリッジグループを指定:EtherIP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 10.0.0.1	
71	exit	
72	!	
73	interface Tunnel 1	Tunnel インタフェース(PPPoE)の設定
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	tunnel mode pppoe profile PPPOE_PROF	
80	pppoe interface gigaethernet 2/1	
81	exit	
82	!	
83	interface Tunnel 2	Tunnel インタフェース(IPsec)の設定
84	tunnel mode ipsec map KYOTEN	
85	exit	
86	!	
87	interface Tunnel 3	Tunnel インタフェース(EtherIP)の設定
88	tunnel mode ether-ip tunnel-profile etherip-prof	Tunnel インタフェースで有効にするEtherIPプロファイルを設定
89	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
90	exit	
91	!	
92	ether-ip tunnel-profile etherip-prof	EtherIPプロファイルの設定
93	tunnel source 10.0.0.1	EtherIPトンネルを確立する自装置(Loopback)IPアドレスの設定
94	tunnel destination 10.0.0.2	EtherIPの通信をする拠点側装置(Loopback)IPアドレスの設定
95	exit	
96	!	
97	pppoe profile PPPOE_PROF	PPPoEの設定
98	account abc012@***.***.ne.jp xxxyyyzzz	
99	exit	
100	!	
101	end	

拠点側FITELnetの設定

	設定例	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	EtherIP対向装置のIPアドレス(Loopback)宛への経路(IPsec Tunnel経由)
8	!	
9	hostname KYOTEN	
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	

All Rights Reserved, Copyright(C) FURUKAWA ELECTRIC CO., LTD. 2020

	設定例	補足
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	VPN通信動作中の詳細なログを残す設定
29	crypto isakmp log sa	
30	crypto isakmp log session	
31	crypto isakmp log negotiation-fail	
32	!	
33	crypto isakmp policy P1-POLICY	ISAKMP ポリシーの設定
34	authentication pre-share	
35	encryption aes	
36	encryption-keysize aes 256 256 256	
37	group 14	
38	lifetime 86400	
39	hash sha	
40	initiate-mode aggressive	
41	exit	
42	!	
43	crypto isakmp profile PROF0001	ISAKMPプロファイルの設定
44	self-identity user-fqdn id-kyoten	
45	set peer 192.0.2.1	
46	set isakmp-policy P1-POLICY	
47	set ipsec-policy P2-POLICY	
48	ike-version 1	
49	local-key SECRET-VPN	
50	exit	
51	!	
52	crypto map CENTER ipsec-isakmp	拠点のVPNピアとのセレクタ情報のエントリー
53	match address SELECTOR	
54	set isakmp-profile PROF0001	
55	exit	
56	!	
57	vlan any 10 20	vlan-id any で対象とするVLAN-ID値を指定。 範囲指定時は、<開始番号>-<終了番号> のように入力する。 例）対象とするVLAN-IDが1234および2000-2005の場合： vlan-id any 1234 2000-2005
58	!	
59	interface GigaEthernet 1/1	GigaEthernet（1/1）インタフェースに、EtherIPトンネルをリンク付け
60	vlan-id any	VLANーIDをANY（1～4094）に指定。 ※対象とするVLAN-IDを基本設定モードのvlan-id anyコマンドで指定可能。指定しない場合は1-4094の全VLAN-IDが対象になるが、設定反映に時間を要する。
61	bridge-group 1	ブリッジグループを指定：EtherIPのTunnelインターフェースで使用するbridge-groupと合わせる
62	exit	
63	!	
64	interface GigaEthernet 1/2	GigaEthernet（1/2）インタフェースに、EtherIPトンネルをリンク付け
65	vlan-id any	VLANーIDをANY（1～4094）に指定。 ※対象とするVLAN-IDを基本設定モードのvlan-id anyコマンドで指定可能。指定しない場合は1-4094の全VLAN-IDが対象になるが、設定反映に時間を要する。
66	bridge-group 1	ブリッジグループを指定：EtherIPのTunnelインターフェースで使用するbridge-groupと合わせる
67	exit	
68	!	
69	interface GigaEthernet 2/1	PPPoE 通信で使用する物理インタフェースの設定
70	vlan-id 2	
71	bridge-group 2	
72	pppoe enable	
73	exit	
74	!	
75	interface Loopback 1	Loopback インタフェースの設定
76	ip address 10.0.0.2	
77	exit	
78	!	
79	interface Tunnel 1	Tunnel インタフェース（PPPoE）の設定
80	description FLETS	
81	ip access-group 100 in	
82	ip access-group 111 in	
83	ip access-group 121 out	
84	tunnel mode pppoe profile PPPOE_PROF	
85	pppoe interface gigaethernet 2/1	
86	exit	
87	!	
88	interface Tunnel 2	Tunnel インタフェース（IPsec）の設定
89	tunnel mode ipsec map CENTER	
90	exit	
91	!	
92	interface Tunnel 3	Tunnel インタフェース（EtherIP）の設定
93	tunnel mode ether-ip tunnel-profile etherip-prof	Tunnel インタフェースで有効にするEtherIPプロファイルを設定
94	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
95	exit	
96	!	
97	ether-ip tunnel-profile etherip-prof	EtherIPプロファイルの設定
98	tunnel source 10.0.0.2	EtherIPトンネルを確立する自装置（Loopback）IPアドレスの設定
99	tunnel destination 10.0.0.1	EtherIPの通信をするセンタ側装置（Loopback）IPアドレスの設定
100	exit	
101	!	
102	pppoe profile PPPOE_PROF	PPPoEの設定
103	account abc345@***.***.ne.jp zzzyyyxxx	
104	exit	
105	!	
106	end	

All Rights Reserved, Copyright(C) FURUKAWA ELECTRIC CO., LTD. 2020