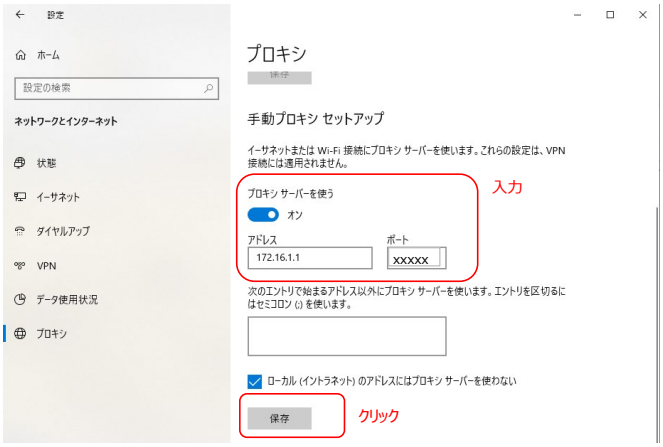
設定例

IPoE網（V4 over V6トンネル）／固定IPサービスでVPN/ローカルブレイクアウト（LBO）を利用する

（対象機種：F70/F71/F220/F221/F220 EX/F221 EX）

概要

IPoE網でVPN接続して構築した社内ネットワーク（Proxy環境下）にて、特定のSaaSを固定IPサービスのV4 over V6トンネル経由でインターネットにブレイクアウトするための設定例です。
・拠点ネットワークの端末にて、Proxyサーバを有効にしてください（例：Windows 10の場合は、下記プロキシ設定を行ってください）。



【注意】
・本設定例にてアプリケーションの基本的な動作確認を行っておりますが、全ての動作を保証するものではございません。
アプリケーションの用途に合わせて、十分に検証を行ってから、ご利用ください。

コマンド設定例

FITELnetの設定
黄色セル：ローカルブレイクアウト機能を利用するために必要な設定です。
赤色セル：VPN機能を利用するために必要な設定です。

	設定例	補足
1	access-list 4001 permit udp ##IPv6 VPNピアアドレス##/128 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 4001 permit 50 ##IPv6 VPNピアアドレス##/128 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	!	
4	no ip route 0.0.0.0 0.0.0.0 tunnel 1	V4overV6トンネル経由のデフォルト経路を削除
5	ip route 0.0.0.0 0.0.0.0 tunnel 2	VPN経由でデフォルトを経路を設定
6	!	
7	local-breakout enable	ローカルブレイクアウトを行う設定
8	local-breakout proxy-server ip any port #LBO対象パケットの宛先ポート番号#	ローカルブレイクアウト対象のプロキシ宛通信のポート番号を設定 （設定されたポート番号を監視してLBO対象かどうかのチェックを行います）
9	local-breakout LBO tunnel 1	ローカルブレイクアウト対象パケットの中継先を設定（V4 over V6 Tunnel）
10	!	
11	lbo-profile LBO	LBOプロファイル設定
12	http-snooping enable with-route	http-snooping機能を有効とする設定。with-routeオプションにより、TCP接続時に宛先アドレスを経路情報として登録して、TCP以外のLBOが可能となります。
13	domain *sample.com	ローカルブレイクアウト対象domainを設定（ブレイクアウト対象のSaaSに合わせて設定してください）
14	exit	
15	!	
16	crypto ipsec replay-check disable	
17	!	
18	crypto ipsec policy IPsec_POLICY	
19	set security-association always-up	
20	set security-association lifetime seconds 28800	
21	set security-association transform-keysize aes 256 256 256	
22	set security-association transform esp-sha512-hmac esp-aes	
23	exit	
24	!	
25	crypto ipsec selector SELECTOR	
26	src 1 ipv4 any	
27	src 2 ipv6 any	
28	dst 1 ipv4 any	
29	dst 2 ipv6 any	
30	exit	
31	!	
32	crypto isakmp keepalive always-send interval 35	
33	crypto isakmp log sa	
34	crypto isakmp log session	
35	crypto isakmp log negotiation-fail	
36	crypto isakmp negotiation always-up-params interval 100 max-initiate 1 max-pending 1 delay 3	
37	!	

	設定例	補足
38	crypto isakmp policy ISAKMP_POLICY	
39	authentication pre-share	
40	encryption aes	
41	encryption-keysize aes 256 256 256	
42	group 15	
43	lifetime 86400	
44	hash sha-512	
45	exit	
46	!	
47	crypto isakmp profile PROF	
48	match identity host IPsec.example.com	
49	local-address source-interface port-channel 1	
50	self-identity user-fqdn CPE@IPsec.example.com	
51	set isakmp-policy ISAKMP_POLICY	
52	set ipsec-policy IPsec_POLICY	
53	set peer ##IPv6 VPNピアアドレス##	
54	ike-version 2	
55	local-key key	
56	exit	
57	!	
58	crypto map MAP ipsec-isakmp	
59	match address SELECTOR	
60	set isakmp-profile PROF	
61	exit	
62	!	
63	interface GigaEthernet 2/1	
64	ipv6 access-group 4001 in	IPv6アクセスリスト紐づけ（VPN許可）
65	exit	
66	!	
67	interface Port-channel ##LAN Port-channel番号##	
68	mss 1350	MSSを設定：LAN回線のMSSをLBO回線よりも小さい値に設定してください ※LANインタフェースのMSSの方が大きいと、TCPセッション変換テーブル作成時に 整合性チェックでエラーして変換テーブルが作成されないことがあります。
69	http-snooping enable	http-snoopingを行うための設定
70	exit	
71	!	
72	interface Tunnel 2	
73	tunnel mode ipsec map MAP	
74	exit	