設定例

ローカルブレイクアウト：Microsoft365（旧Office365）エンドポイント情報を使う
対象装置：FITELnet F70/F71/F220/F221/F220 EX/F221 EX

概要

Microsoft365エンドポイント情報を取得して、LBO経路として登録して、ローカルブレイクアウト通信を行うための設定例です。
次の1)-3)の動作により、端末からMicrosoft365エンドポイントへのLBO通信が可能となります。

1）拠点はendpoints.office.comのアドレスをDNSサーバに問い合わせてアドレス解決します。その後、https://endpoints.office.com/endpoints/worldwide より、Microsoft365エンドポイント情報を取得します（デフォルト経路向：センタ機経由で上記URLにアクセス）。

2) 拠点は、Microsoft365エンドポイント情報に記載されている"ips"を、LBO経路として登録します。

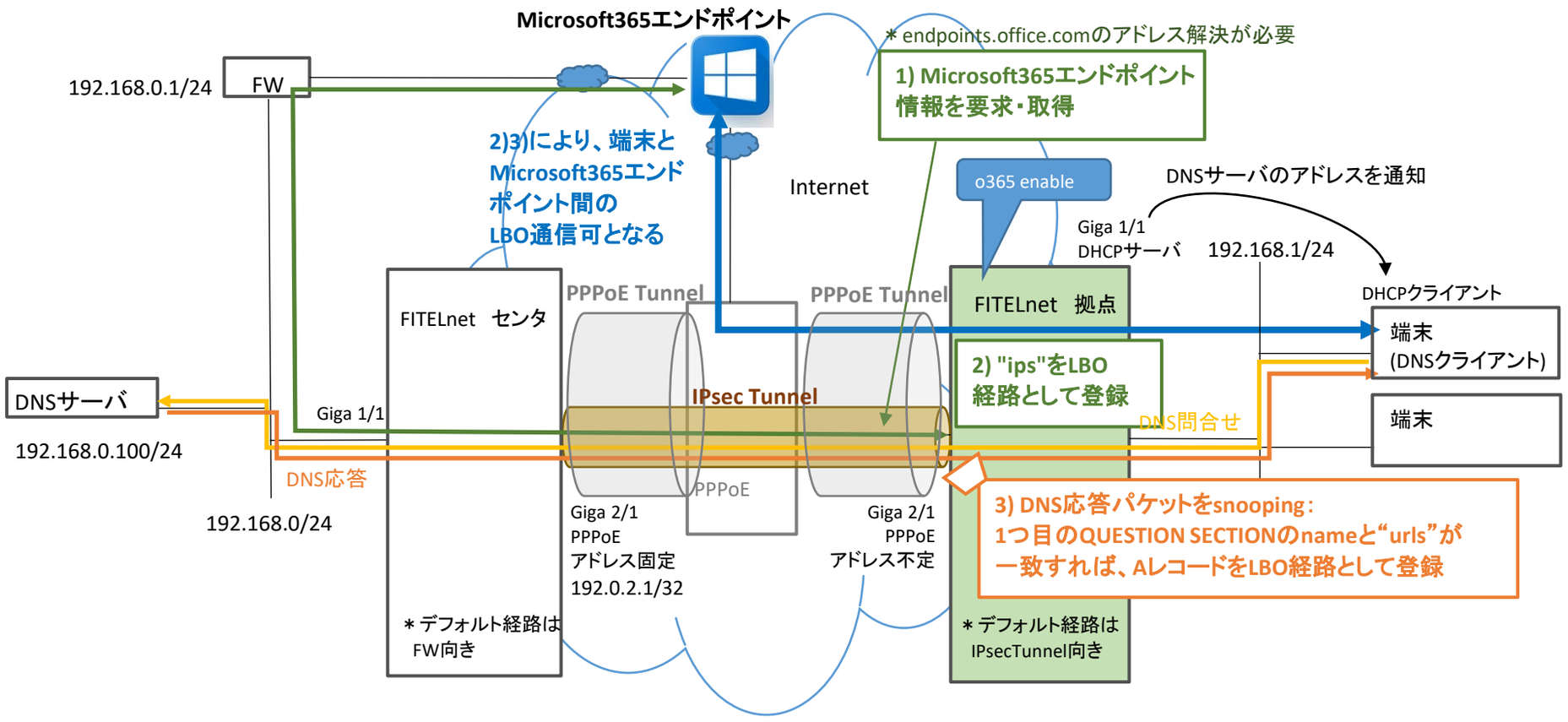
3）端末が通信開始しようとしてDNSサーバへアドレスを問い合わせた際に、拠点はDNSサーバが端末宛に送信したDNS応答パケットをsnoopingします。
DNS応答パケットに書かれた1つ目のQUESTION SECTIONのnameが、Microsoftエンドポイント情報に記載されている"urls"と一致すれば、拠点はnameに対応するAレコード（IPv6の場合はAAAAレコード）をLBO経路として登録します。

・Microsoft365エンドポイント情報取得について：
1) のMicrosoft365エンドポイント情報取得は、装置起動時および定期取得のタイミングにて行われます。定期取得間隔はデフォルトで86400秒ですが、o365 updateコマンドにより変更可能です。

・LBO経路削除契機について：
2)の"ips"により登録されたLBO経路は、Microsoft365エンドポイント情報取得時に、"ips"が消えている場合に削除します。
3)のDNS応答パケットにより登録されたLBO経路は、dns-snooping expire設定時間（デフォルト86,400秒）保持、
DNS応答パケットのANSWER SECTIONに記載のTTL時間がdns-snooping expire以上であれば、TTL時間満了まで保持します。
（上記タイマ動作は、F70/F71：V01.02以降、F220/F221：V01.04以降の動作となります）
2), 3)どちらのLBO経路とも、o365 enable設定削除等でローカルブレイクアウト対象ドメインで無くなった場合には削除します。

下記説明資料の6ページを合わせてご確認ください。
ローカルブレイクアウト説明資料

Windows Update / Microsoft Update のLBOを併用する際には、拠点側FITELnetに下記設定例と同様にdomain設定を追加してください。
ローカルブレイクアウト：Windows Update / Microsoft Update



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	!	

	設定例（センタ）	補足
6	ip route 0.0.0.0 0.0.0.0 192.168.0.1	Default経路(FW経由)
7	ip route 192.168.1.0 255.255.255.0 tunnel 2	拠点LAN宛てStatic経路(IPsec Tunnel経由)
8	ip route 192.168.1.0 255.255.255.0 null 0 250	IPsec Tunnelダウン時に拠点LAN宛てパケットを破棄する設定
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-sha256-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	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	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)
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-256	
41	initiate-mode aggressive	
42	exit	
43	!	
44	crypto isakmp profile PROF0001	ISAKMPプロファイルの設定
45	match identity user id-kyoten	
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 map KYOTEN ipsec-isakmp	拠点のVPNピアとのセレクタ情報のエントリー
54	match address SELECTOR	
55	set isakmp-profile PROF0001	
56	exit	
57	!	
58	interface GigaEthernet 1/1	GigaEthernet インタフェースに、port-channel をリンク付け
59	vlan-id 1	
60	bridge-group 1	
61	channel-group 1	
62	exit	
63	!	
64	interface GigaEthernet 2/1	PPPoE 通信で使用する物理インタフェースの設定
65	vlan-id 2	
66	bridge-group 2	
67	pppoe enable	
68	exit	
69	!	
70	interface Port-channel 1	Port-channel にLAN側IPアドレスを設定
71	ip address 192.168.0.254 255.255.255.0	
72	mss 1300	
73	exit	
74	!	
75	interface Tunnel 1	Tunnel インタフェース（PPPoE）の設定
76	description FLETS	
77	ip address 192.0.2.1 255.255.255.255	
78	ip access-group 100 in	
79	ip access-group 111 in	
80	ip access-group 121 out	
81	tunnel mode pppoe profile PPPOE_PROF	
82	pppoe interface gigaethernet 2/1	
83	exit	
84	!	Tunnel インタフェース（IPsec）の設定
85	interface Tunnel 2	
86	tunnel mode ipsec map KYOTEN	
87	link-state sync-sa	
88	exit	
89	!	
90	pppoe profile PPPOE_PROF	PPPoEの設定
91	account abc012@***.***.ne.jp xxxyyyzzz	
92	exit	
93	!	
94	end	

拠点側FITELnet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 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 192.0.2.1 255.255.255.255 tunnel 1	センタPPPoEIFへの経路(PPPoE経由）
7	ip route 0.0.0.0 0.0.0.0 tunnel 2	Default経路(IPsec Tunnel経由）
8	ip name-server 192.168.0.100	DNSサーバアドレスの設定(endpoints.office.comのアドレス解決用)
9	ip name-server source-interface port-channel 1	DNSサーバへの問い合わせ時の送信元アドレスの設定
10	ip nat list 1 192.168.1.0 0.0.0.255	NATの設定
11	!	
12	ip dhcp server-profile lan1	DHCP サーバ機能を利用する設定
13	address 192.168.1.1 192.168.1.200	配布IPアドレスの範囲
14	lease-time 28800	DHCPリース期間(秒）
15	dns 192.168.0.100	プライマリDNSサーバIPアドレス
16	gateway 192.168.1.254	デフォルトルータのIPアドレス
17	exit	
18	!	
19	crypto ipsec policy P2-POLICY	IPSECポリシーの設定
20	set pfs group14	
21	set security-association always-up	
22	set security-association lifetime seconds 28800	
23	set security-association transform-keysize aes 256 256 256	
24	set security-association transform esp-aes esp-sha256-hmac	
25	set mtu 1454	
26	set ip df-bit 0	
27	set ip fragment post	
28	exit	
29	!	
30	crypto ipsec selector SELECTOR	VPNセレクタの設定
31	src 1 ipv4 any	
32	dst 1 ipv4 any	
33	exit	
34	!	
35	crypto isakmp keepalive	KeepAlive機能として使用するDPDの設定
36	logging level informational	VPN通信動作中の詳細なログを残す設定
37	crypto isakmp log sa	
38	crypto isakmp log session	
39	crypto isakmp log negotiation-fail	
40	!	
41	hostname KYOTEN	
42	!	
43	crypto isakmp policy P1-POLICY	ISAKMP ポリシーの設定
44	authentication pre-share	
45	encryption aes	
46	encryption-keysize aes 256 256 256	
47	group 14	
48	lifetime 86400	
49	hash sha-256	
50	initiate-mode aggressive	
51	exit	
52	!	
53	crypto isakmp profile PROF0001	ISAKMPプロファイルの設定
54	self-identity user-fqdn id-kyoten	
55	set isakmp-policy P1-POLICY	
56	set ipsec-policy P2-POLICY	
57	set peer 192.0.2.1	
58	ike-version 1	
59	local-key SECRET-VPN	
60	exit	
61	!	
62	crypto map CENTER ipsec-isakmp	センタのVPNピアとのセレクタ情報のエントリー
63	match address SELECTOR	
64	set isakmp-profile PROF0001	
65	exit	
66	!	
67	interface GigaEthernet 1/1	GigaEthernet インタフェースに、port-channel をリンク付け
68	vlan-id 1	
69	bridge-group 1	
70	channel-group 1	
71	exit	
72	!	
73	interface GigaEthernet 2/1	PPPoE 通信で使用する物理インタフェースの設定
74	vlan-id 2	
75	bridge-group 2	
76	pppoe enable	
77	exit	
78	!	
79	interface Port-channel 1	Port-channel にLAN側IPアドレスを設定
80	ip address 192.168.1.254 255.255.255.0	
81	ip dhcp service server	DHCPサーバ機能を有効化
82	ip dhcp server-profile lan1	DHCPサーバ機能で使用するプロファイルの指定
83	mss 1300	
84	exit	
85	!	

	設定例（拠点）	補足
86	interface Tunnel 1	Tunnel インタフェース（PPPoE）の設定
87	description FLETS	
88	ip access-group 100 in	
89	ip access-group 111 in	
90	ip access-group 121 out	
91	ip nat inside source list 1 interface	
92	tunnel mode pppoe profile PPPOE_PROF	
93	pppoe interface gigaethernet 2/1	
94	exit	
95	!	
96	interface Tunnel 2	Tunnel インタフェース（IPsec）の設定
97	tunnel mode ipsec map CENTER	
98	dns-snooping enable	dns-snooping機能を有効とする設定
99	exit	
100	!	
101	pppoe profile PPPOE_PROF	PPPoEの設定
102	account abc345@***.***.ne.jp zzzyyyxxx	
103	exit	
104	!	
105	local-breakout enable	ローカルブレイクアウトを行う設定
106	local-breakout LBO1 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
107	!	
108	lbo-profile LBO1	LBOプロファイル設定
109	o365 enable	ローカルブレイクアウト対象トラフィックとしてMicrosoft 365のトラフィックを有効とする設定
110	dns-snooping enable	dns-snooping機能を有効とする設定
111	exit	
112	!	
113	end	